Proskauer

Government Enforcement

June 2023

The last webinar in our series concerned AI and government enforcement. Companies are currently gauging how government will focus enforcement efforts in this new, emerging area by looking to a few guideposts. The first is the FTC, which has released specific guidance and rules that refers to AI tools. Other agencies have at least indicated their interest in oversight, including the DOJ, CFPB and the EEOC, and it is expected that there will be more to come from these agencies and others, including state agencies involved with, for example, financial services. With few existing regulations on AI, the presenters expect to see regulation-by-enforcement of these existing laws that will shape the regulatory environment concerning AI. The presenters predicted that future enforcement in this area might be seen in multiple areas, including consumer protection, cases dealing with bias and discrimination, cybersecurity, securities fraud, and antitrust.

FTC Guidelines

According to the presenters, the FTC has thus far been the most proactive regulator with respect to issuing AI-related guidance. The FTC's enforcement authority extends to several statutes that are relevant to AI: the FTC Act, the Fair Credit Reporting Act and the Equal Credit Opportunity Act. The presenters noted that the FTC Act, covering unfair and deceptive trade practice, can extend to a broad range of regulatory scenarios; the Fair Credit Reporting Act can cover instances where an algorithm is used to deny people employment, housing, insurance, credit, etc.; and the Equal Credit Opportunity Act makes it illegal for a company to use biased algorithms that result in discrimination based on a variety of protected categories.

In 2020, the FTC released its initial guidance on AI, emphasizing transparency where consumers were the focal point and stressing the need for companies to be clear about their decisions surrounding the use of AI. In 2021 an FTC guidance encouraged marketers to harness the benefits of AI without "inadvertently introducing bias or other unfair outcomes." To avoid this issue, the agency stressed the need for companies to regularly test AI products for bias and to ensure they are working as designed. It further stressed that compliance would require transparency as to how AI product works, how its dataset it is trained or fine-tuned, and the way an AI product collects data. The presenters commented that while this approach may not necessarily align with companies trying to develop proprietary technologies, they stated that, from the FTC's perspective, the benefits of transparency can help the marketplace ferret out flaws in AI products and methodologies. The presenters also noted that the FTC has, in many instances, cautioned companies not to exaggerate the capabilities of emerging technologies such as AI. As the presenters noted, to remain compliant under the FTC Act and other statutes, it is important to be objective about what a product can and cannot deliver.

In February 2023 the FTC released its most recent pronouncements on AI, specifically focusing on the way companies advertise and market products to consumers, and reminding companies to avoid making false or unsubstantiated claims about an AI product's functionality. The FTC suggested companies ask themselves multiple questions, including "Are you exaggerating what your AI product can do?", "Are you aware of the risks?" and "Does the product actually use AI at all?" The guidance also asked: "Are you promising that your AI product does something better than a non-AI product?" The presenters noted that it is important to recognize that the FTC and other enforcement agencies can scrutinize what is behind such statements. As to the risks, the presenters stated that the FTC will look to see if companies have conducted reasonable diligence and considered reasonably foreseeable risks in the way its product is going to be used and how it might impact consumers and others in the marketplace.

Joint Statement by Federal Agencies (FTC, DOJ, CFPB, EEOC)

AI has also garnered the attention of other regulators. For example, in April 2023 the FTC, DOJ, CFPB and EEOC issued a joint statement, "Enforcement Efforts Against Discrimination and Bias in Automated Systems." The document outlined each agency's commitment to enforce existing legal and regulatory authority to ensure responsible innovation in the AI space and noted that AI products may be used by public and private entities to make critical decisions that impact individuals' rights and opportunities yet have the potential for biased outcomes. The agencies highlighted certain areas of particular interest, including: data and datasets (i.e., the potential for skewed results from inaccurate information), model opacity (i.e., the "black box" issue) and design and use (i.e., if the developer does not account for how the tool can be used or make flawed assumptions about use) The presenters interpreted the statement to mean that action surrounding these issues should be expected in the future and that agencies will be using existing laws to root out what it deems unlawful acts or outcomes, regardless of what technologies are used and regardless of the complexity of such AI technologies.

Potential Areas of AI-Related Enforcement -- Consumer Protection

With respect to consumer protection enforcement, the presenters pointed to three areas of potential focus: consumer disclosures and transparency; the use of AI in the provision of financial services; and discrimination in lending caused by non-transparent algorithms. For example, the SEC has expressed interest in oversight of the use of AI for such things as automated trading and wealth management tools; the presenters also mentioned the DOJ, in conjunction with other federal agencies expressing their intention to scrutinize black box-type underwriting algorithms where the outcomes can have disparate impact on protected classes or otherwise create unfair or misleading results. Consumer protection enforcement could come into play, according to the presenters, as it relates to the capacity of generative AI to produce false and misleading information. For example, the presenters noted that there is a risk that employees of a company might blindly might rely on generative AI tools to produce inaccurate and unverified work product that could end up in public disclosures or marketing statements directed to consumers, potentially exposing the company to enforcement.

Potential Areas of AI-Related Enforcement – Bias and Discrimination

The DOJ's civil rights division has been working to address concerns with bias and discrimination in AI systems. For example, the presenters pointed to a prior DOJ investigation involving use of a health insurer's algorithm that had inadvertently produced treatment decisions that were inequitable to black patients. The presenters noted that one takeaway from the investigation is that existing anti-discrimination laws do not require a level of scienter and enforcement of such laws might seek to redress an AI system's disparate impact or unequal treatment, despite a developer or provider having the best of intentions when developing or using an AI product, particularly a generative AI in a healthcare setting. Thus, the presenters noted that developers and providers should think about the potential consequences and regulatory risk for bias and discrimination, particular in fields where inaccurate or biased outcomes that can have substantial effects on individuals, such as healthcare or housing.

Potential Areas of AI-Related Enforcement – Cybersecurity

Cybersecurity has been a major focus on multiple federal and state regulators for some time now and the increased use of AI will introduce new concerns and issues. For example, in the recently released SEC proposal for new rules addressing cybersecurity risks to U.S. securities markets, the SEC noted that market entities are increasingly relying on information systems to provide services and such reliance turns them into targets for hackers and cyberthieves. Related to these concerns, the presenters noted that the increasing use of AI creates these same vulnerabilities and is related to how some of the new generative AI tools work (e.g., generative AI prompts stored in the cloud and potentially vulnerable to hackers) and if new SEC standards are issued, companies using AI tools might have to account for how the information is safeguarded, how the company limits the number of employees with access to such tools and what procedures are in place to protect confidential information from being submitted into an AI product.

Potential Areas of AI-Related Enforcement – Securities Fraud

In recent months, headlines have been replete with stories about how capital has been pouring into AI start-ups. The presenters noted that, with all the hype, there is often a mismatch between opportunities and the dollars chasing them, which can, in some cases, lead to instances of fraud, likely prompting future SEC and DOJ actions. This realization is not only true for unscrupulous operators, but also the reckless, both of whom could be targets of securities fraud actions. Thus, as noted by the presenters, statements and disclosures to investors and the marketplace about the state of a product, its capabilities, and a company's development state should be made cautiously when made in conjunction with fundraising or selling securities. Moreover, the presenters pointed out that if a company relies on a generative AI product, which has produced an inaccurate output, and uses such content to make material misstatements to the public or investors in connection with a security, such company could conceivably be deemed reckless under the law (particularly in view of the disclaimers displayed by generative AI products about inaccurate responses and content). The presenters pointed out that companies are at risk from the use of generative AI by employees without proper procedures, supervision or vetting processes governing use and approval of such AI content.

Potential Areas of AI-Related Enforcement – Antitrust Concerns

This is another area where the presenters expect future enforcement, specifically where AI algorithms are seen to promote price fixing or collusion. AI algorithms can be used by companies to coordinate their activities, even if unintentionally. It should be recalled that AI algorithms are always learning and it is possible that such programs might unwittingly produce anti-competitive effects without coordination with other companies that may be using similar pricing algorithms. The presenters noted that DOJ is already focused on the potential anti-competitive effects of AI and is prepared to use scientific and other resources to investigate potential violations.

Related Professionals

- **Seetha Ramachandran**
  Partner