Strategic Perspectives

As AI usage soars, academics, legal experts look for regulation blueprints

By Suzanne Cosgrove

Although major industries ranging from finance to health care to film production are scurrying to implement artificial intelligence (AI) applications – embracing its promise of faster, better outcomes – the regulation of AI technology is still in its infancy. To push the effort along, academics and legal experts are drawing up proposals that promote basic standards and principles to guard against its misuse.

Legislators and regulators, in turn, seem to agree that the need for an innovative set of new rules is great. In a unique show of cooperation, last week the U.S. House announced the formation of a bipartisan task force on artificial intelligence, led by Congressmen Ted Lieu (D-Calif.) and Jay Obernolte (R-Calif.).

Recent efforts to corral AI include:

- A White House Executive Order, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- A bipartisan congressional task force on artificial intelligence, led by Reps. Ted Lieu and Jay Obernolte.
- The DOJ's Office of Legal Policy, which is developing a team of technical and policy experts in the field.
- The CFTC's request for comment (RFC) on the uses and risks of AI in regulated derivatives markets.

Separately, the DOJ has appointed Jonathan Mayer, a professor at Princeton University's Department of Computer Science and School of Public and International Affairs, as the DOJ's first chief science and technology advisor and chief AI officer. "The Justice Department must keep pace with rapidly evolving scientific and technological developments in order to fulfill our mission to uphold the rule of law, keep our country safe, and protect civil rights," said U.S. Attorney General Merrick B. Garland, in a press statement.

Further, in January the CFTC's Divisions of Market Oversight, Clearing and Risk, Market Participants, and Data and the Office of Technology Innovation put out a request for comment (RFC) on current and potential uses and risks of artificial intelligence in CFTC-regulated derivatives markets. The Commission's RFC seeks the public's input on the definition of AI and its applications, including its use in trading, risk management, compliance, cybersecurity, recordkeeping, data processing and analytics and customer interactions.

And last fall, the White House issued an Executive Order, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which advanced the development and use of AI in accordance with eight guiding principles and priorities, including the protection of privacy and civil liberties.

Calls for a novel approach. The challenges to financial stability that AI may pose in the future will require new thinking on systemwide or macro-prudential policy interventions, said SEC Chair Gary Gensler, in a February 13 address at the Yale Law School.

While AI "opens up tremendous opportunities for humanity," current model risk management guidance, "generally written prior to this new wave of data analytics," will need to be updated, it won't be sufficient, Gensler said.

The SEC chair noted AI already is used in finance, citing its prominence in call centers, compliance programs and claims processing. The technology also has fueled rapid change in the field of robo advisors and brokerage apps, but with those opportunities come challenges, at both the micro and macro level, he said.

Bad actors have a new tool, AI, to exploit the public. "So what happens when you combine AI, finance, and the law of fraud?" Gensler asked his Yale audience.

Standards of care. At a February 16 symposium on "AI and the Law" at the Northwestern Pritzker School of Law, Bryan Choi, an Ohio State University law professor, observed that current approaches to AI regulation have embraced an *ex ante* risk regulation approach. But a closer examination shows that these broad, horizontal efforts are thin on substantive details and delegate much of the effort to industry self-regulation, he said.

"Ex *post* tort liability approaches will have to defer to 'professional judgment' and self-regulation unless a consensus standard of care can be established," Choi said.

In a recent paper titled "AI Malpractice," published by the DePaul Law Review, Choi explored the idea that AI modelers should be held to a professional standard of care. "Recent scholarship has argued that those who build AI systems owe special duties to the public to promote values such as safety, fairness, transparency, and accountability," he said. "Yet, there is little agreement as to what the content of those duties should be. Nor is there a framework for how conflicting views should be resolved as a matter of law."

The customary care standard offers a more flexible approach that tolerates a range of professional practices above a minimum expectation of competence, Choi noted. This approach often is adopted for occupations like software development, where the science of the field is hotly contested or is rapidly evolving. Although it is tempting to treat AI liability as a simple extension of software liability, there are key differences, he writes.

The first key difference is that AI work has not yet become essential to the social fabric the way software services have, so the risk of underproviding AI services is less troublesome, Choi said. Secondly, deep-learning AI techniques differ significantly from conventional software development practices in ways that will facilitate convergence and uniformity in expert knowledge. Those variances suggest that the law of AI liability will chart a different path than the law of software liability, he suggested.

For the immediate term, a strict liability approach is most appropriate, Choi said. In the longer term, as AI becomes integrated into ordinary society, courts should expect to transition away from strict liability. For aspects that elude expert consensus and require exercise of discretionary judgment, courts should favor the professional malpractice standard. If there are broad areas of AI work where experts can come to agreement on baseline standards, courts then can revert to the default of ordinary reasonable care.

Current oversight. Thus far, public oversight is largely routed through private governance and self-regulation mechanisms, Choi said. The leading effort has been the AI Risk Management Framework, issued by the National Institute of Standards and Technology (NIST), which invites enterprises to engage in voluntary self-assessments of risk.

In addition, the European Union has adopted the EU AI Act, which categorizes AI systems as "limited risk," "high-risk," or "unacceptable risk," and then seeks to calibrate compliance obligations accordingly. Those obligations have been outsourced to private standard-setting organizations and have yet to be written.

Issues in finance. AI raises a host of issues that aren't new but are accentuated by it, Gensler noted in his speech. "First, AI models' decisions and outcomes are often unexplainable. Second, AI also may make biased decisions because the outcomes of its algorithms may be based on data reflecting historical biases. Third, the ability of these predictive models to predict doesn't mean they are always accurate."

"Though parts of our securities laws have standards of strict liability, such as conducting an unregistered offering, many of the key anti-fraud sections of the 1933, 1934, and 1940 acts require some form of intent or at least negligence," Gensler said. "Did somebody knowingly or recklessly do something? Were they negligent?"

Gensler pointed to a paper by Robin Feldman and Kara Stein, "AI Governance in the Financial Industry," which suggests little space exists in current legal and regulatory systems to properly manage the actions of artificial intelligence in the financial space.

Artificial intelligence does not "have intent," the paper states, and therefore cannot form the scienter required in many securities law contexts. It also defies the approach commonly used in financial regulation of focusing on size or sophistication. "Moreover, the activity of artificial intelligence is too diffuse, distributed, and ephemeral to effectively govern by aiming regulatory firepower at the artificial intelligence itself or even at the entities and individuals currently targeted in securities law."

Harm, not intent. Gensler noted the Feldman-Stein paper addresses programmable harm, predictable harm, and unpredictable harm.

The first, programmable harm, is straightforward: if you use an algorithm and are optimizing it to manipulate or defraud the public, which is fraud, he said. The second category, predictable harm, is also reasonably straightforward. "Have you had a reckless or knowing disregard of the foreseeable risks of your actions, in this case, deploying a particular AI model? Did you act reasonably? "

The third category asks how one holds liable the persons who deploy the AI models that create truly unpredictable harm. "Some of that will play out in the courts," Gensler said. "Right now, though, the opportunities for deception or manipulation most likely fall in the programmable and predictable harm categories rather than being truly unpredictable."