GIBSON DUNN

AI Risks Guide Sets Starting Point for Compliance, Regulation

In the Media | February 1, 2023

Bloomberg Law

Related People

Cassandra L. Gaedt-Sheckter

The latest government guidance addressing artificial intelligence risks serves as a launch pad for compliance considerations and could signal regulatory and lawmaker action to come, attorneys say.

AI technology is being implemented across the business universe, for tasks such as resume screening and generating art, text, and computer code. With its rapid growth and adoption comes the potential for unintentional algorithmic discrimination and violations of intellectual property and other laws.

The AI Risk Management Framework, released Jan. 26 by the National Institute of Standards and Technology, offers the most comprehensive approach to date that companies can use to assess and manage the myriad risks associated with the implementation or development of AI, attorneys who advise clients on the technology said.

The NIST framework establishes a common language to understand and discuss AI issues for businesses and lawyers, and it offers insight into the government's views on the fast-evolving technology that attorneys predict will drive an influx of regulation and legislation in coming years.

"It provides some plain-language guidance that I can hand over to a client to accompany the legal guidance that I might be giving them. It also, frankly, is a harbinger of things to come from the regulatory perspective," said Kathleen McGee, a partner in Lowenstein Sandler LLP's technology practice who previously headed the Bureau of Internet and Technology of the New York state Attorney General's Office.

The framework, created by mandate in the fiscal year 2021 National Defense Authorization Act, outlines considerations that companies should take into account when measuring and assessing risks posed by AI. It also focuses on the structures a business can use to mitigate them.

However, the principles detailed in the framework—which the agency explicitly calls "non-sector specific and use-case agnostic"—may be viewed as too abstract by some, and it will take time to see how companies and practitioners adopt them in daily operations, attorneys said.

Risks, Benefits

Artificial intelligence, if left unchecked, has the potential to harm people, organizations, and even ecosystems, according to NIST's framework.

AI can perpetuate systemic biases against individuals in certain demographic groups, enhance rising cybersecurity threats companies face, and disrupt the global financial system, the framework said.

The technology has already received regulatory, legal, and academic attention for concerns over employment discrimination, intellectual property violations, and cybersecurity threats.

NIST noted that many threatening manifestations of AI are yet to be discovered, underlining that its framework was designed with the flexibility to “address new risks as they emerge.”

Despite the risks associated with the technology, both the agency and attorneys emphasized that well-designed and well-governed AI can benefit companies and society by enhancing efficiency.

AI Compliance and Regulation

NIST was methodical in its approach to developing the AI framework, releasing two draft versions over the course of two years and seeking feedback from interested parties including industry, academia, and government voices. That resulted in the most comprehensive guidance on AI so far, one which serves as a useful tool to head off prescriptive laws and regulation in the future, attorneys said.

The framework is oriented around four basic principles: govern, map, measure, and manage.

“Govern” outlines basic considerations for building an internal structure of assigned responsibility and processes, the manage function establishes how resources should be allocated to mitigate the risks identified by mapping and measuring, according to the framework.

NIST’s focus on governance and management can help attorneys and clients understand how to put data they collect to use, and it underlines the need for identifying leaders who understand an AI technology enough to make appropriate decisions when a risk is identified internally, said Natasha Allen, Foley & Lardner LLP’s AI group co-chair.

The map function emphasizes the importance of documenting the segmented parts of an AI system to holistically understand how it operates, and “measure” encourages developers and implementers of AI to quantify the risks a technology could pose.

While the high-level ideas discussed in the framework may be too broad to easily apply to specific clients, the accompanying draft playbook includes more useful actionable suggestions, said Cassandra Gaedt-Sheckter, the co-chair of Gibson, Dunn & Crutcher LLP’s AI practice.

“It seems to be a helpful guide to navigating those four pillars or functions into actual practical design and development and deployment. I think, depending on the type of learner you are, it’s important to see examples and see practical applications of the framework,” Gaedt-Sheckter said.

The playbook will help Gaedt-Sheckter flesh out assessments of legal and societal risks that arise from AI technology, the results of which determine where companies prioritize their attention, she said.

A notable suggestion detailed in the framework’s playbook is to map out all of the third-party software and data an AI system relies on, Allen said. This allows companies to identify risks—such as biased data or insecure software—and how the third parties are mitigating them, she said.

Allen said she views the framework as a way for government figures to test the waters for developing laws by mandating NIST to develop a resource built on the insight of professionals who interact with complex AI technology every day.

Active regulators with the bandwidth and technical acumen are also going to start examining the impacts of AI, especially in the contexts of investor and consumer concerns, said McGee.

“I think you can expect them to turn to things like this NIST framework for action plans, really, on how to evaluate whether or not a particular entity becomes a target,” she said.

‘Balls and Strikes’

However, the framework doesn’t answer enough practical questions that clients are already raising as they intertwine AI technology into their operations, said Avi Gesser, co-chair of Debevoise & Plimpton LLP’s data security group.

Some companies, for example, are using AI to monitor the tone of customer service call complaints, which raises challenging questions about privacy and culture that NIST’s work doesn’t easily answer, Gesser said.

Gesser called the guidance a useful “issue-spotting document” that his firm may use to evaluate its existing AI compliance program.

“But for the practitioners, right, like if NIST after two years isn’t willing to make the tough choices about what is good or what is bad, how am I supposed to call balls and strikes here?” Gesser said.

Other AI attorneys also underlined the challenges presented by the lack of specific detail contained in the framework.

“It’ll take some time for all the practitioners and businesses to really dig in and digest it,” Gaedt-Sheckter of Gibson Dunn said.

The framework isn’t a checklist that companies developing or implementing AI can instantly adopt, and a lot is left to interpretation, said Brad Fisher, the CEO of AI company Lumenova.

That lack of specificity seems intentional on NIST’s part, with the framework noting that it provides “flexibility to organizations of all sizes and in all sectors.”

Another challenge presented by the framework is its voluntary nature, attorneys said.

Companies are aware that more laws and regulations governing AI are likely to come, so aligning their systems with a government-backed framework is a useful way to stay on top of what comes later, they said.

“The mistake, I think is to think that this is optional,” Gesser said.

Reproduced with permission. Copyright February 1, 2023, Bloomberg Industry Group 800-372-1033 https://www.bloombergindustry.com

Related Capabilities

Artificial Intelligence