LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

AI Governance Insights For Companies After Senate Hearing

By **Dominique Shelton Leipzig, Paul C. de Bernier and Brad Peterson** (July 31, 2023, 5:17 PM EDT)

Recently, the U.S. Senate Judiciary Subcommittee on Privacy and Technology held its first hearing on artificial intelligence, which featured witness testimony from Sam Altman, the CEO of OpenAI, Christina Montgomery, the chief privacy officer at IBM Corp., and Gary Marcus, a professor emeritus at New York University.[1]


Dominique Shelton Leipzig

The hearing — "Oversight of AI: Rules for Artificial Intelligence" — showed an emerging consensus among the senators on both sides about the risks of uncontrolled AI and the need for and general direction of future regulation of AI.

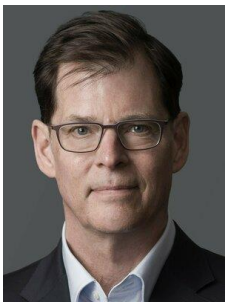
The impetus for the May hearing was, of course, the now-widespread use of generative AI — that is, AI that creates new content using machine learning and neural networks.


Paul C. de Bernier

New powerful generative AI models have increased — by orders of magnitude — the number of users of AI and, thus, the risk to both users and society.

A key theme of the hearing was acknowledging that previous legislation failed to regulate AI in a timely manner. For example, social media had caused great harm, and a similar failure with AI could cause still greater harm.

Calls for Regulation, Best Practices and Other Issues at the Hearing


Brad Peterson

Altman called for greater regulation of AI,[2] including creating a new safety and licensing agency, developing compliance and safety standards, and requiring independent audits of companies:

> OpenAI believes that regulation of AI is essential, and we're eager to help policymakers as they determine how to facilitate regulation that balances incentivizing safety while ensuring that people are able to access the technology's benefits ... [It] is vital that AI companies — especially those working on the most powerful models — adhere to an appropriate set of safety requirements, including internal and external testing prior to release and publication of evaluation results. To ensure this, the U.S. government should consider a combination of licensing or registration requirements for development and release of AI models above a crucial threshold of capabilities, alongside incentives for full compliance with these requirements.

Montgomery emphasized the need for targeted, incremental regulation based upon specific AI uses rather than blanket regulation of AI technology.

While she argued for clearer regulatory guidance for AI developers, she did not argue for a separate AI agency. Instead, she focused on the existing agencies that have identified their intention to enforce.

Finally, she emphasized that companies should act now and not wait for legislation to engage in the trustworthy AI practices that IBM has embraced, such as testing for accuracy, bias, transparency and explainability.

She acknowledged, however, that IBM models are primarily oriented toward business-to-business applications rather than consumer-facing ones and advocated for the implementation of a reasonable care standard to establish accountability for AI systems.

Montgomery reported on IBM's internal governance framework, which includes a designated AI officer, an ethics board, impact assessments, disclosure of data sources, and user notification when engaging with AI.

Marcus argued for engaging the scientific community in developing standards for testing of AI and proposed an increase in funding for research focused on the safety of AI. He also called for a global approach and pointed out some of the harms that can occur, such as AI encouraging users to take their own life, and cybersecurity risks, if AI regulation does not occur.

He made the case that the current court system may not be equipped to effectively regulate AI technology and stressed the importance of robust oversight by a governing agency. He argued for the creation of a safety-review board, such as the U.S. Food and Drug Administration, including the ability to recall AI products.

Emerging AI Consensus From Senators and Potential Insights Into the Direction of Future Regulation

The senators appeared remarkably aligned across party lines. The following broad areas had at least some bipartisan support:

1. Regulatory Oversight

- An independent agency/commission to oversee AI; and
- An AI ethics board to ensure AI encourages faith in societal and democratic values.

2. AI Testing, Regulatory Licenses, and Audits

- Predeployment testing;
- Post-deployment audits, monitoring and testing of AI for accuracy, children's safety, cyber resilience, among other areas; and
- Licensing of AI, and revocation of licenses where AI fails post-deployment testing and monitoring thresholds.

3. Company Risk Assessments and Mitigation

- Risk assessments to determine areas for risk mitigation; and
- Focus areas for pre- and post-deployment risk assessments to include, for example:
    - Equitable treatment of diverse groups and avoiding bias;
    - Privacy risks if training data includes personal information;
    - Misinformation, hallucinations or inaccurate AI;
    - Rights of content providers and other intellectual property owners in data used to train AI systems models;
    - Potential use of AI to impersonate voice, likeness or style;
    - Cybersecurity;
    - National security; and
    - Ability of AI to shape public opinion and/or influence elections and voting.

4. Transparency to Citizens When Interacting With AI and Explainability of Models

- Self-disclosed "nutrition labels" that would explain, based on risk assessments, how or how not to rely on AI in certain contexts;

- Notice to individuals when they are interacting with AI; and

- Need for trust and transparency pertaining to AI.

5. International Leadership

- Global coordination and leadership by the U.S. to avoid circumstances where U.S. companies are inhibited by regulation in a manner greater than non-U.S. competitors and non-U.S. actors can persist with unapproved practices; and

- Regulating generative AI now and not being too late to provide guidance and avoid harm.

Practical Takeaways for AI Developers and Users, Including Boards of Directors

The U.S. appears headed toward regulating at least generative AI and perhaps other AI uses. This regulation is likely to follow the themes of the 1,000+ pages of draft and existing legislation around the world and states in the U.S. that have already published AI-specific laws and guidance.

Based on the themes during the hearing, we recommend that companies consider the following steps to prepare for anticipated regulatory developments:

AI Governance

Set up a team to lead AI efforts and document an AI governance program.

As part of that program, understand whether and how your internal organization and service providers are using AI and how that might impact your compliance burdens and IP rights.

Take an approach specific to your business and likely use cases, and develop organizational standards to comply with anticipated regulations and avoid yet-to-be regulated harm to citizens. Institute review of

all AI initiatives to only implement AI with well-considered use cases that are consistent with anticipated regulations.

The goal here is not to limit innovation, but to channel it into areas that will remain legal — and thus provide a return on the investment.

Data Governance

Inventory your training data and maintain copies so that you can document what data each version of your AI systems was trained on. Verify that you have contractual and legal rights to use the data as training data.

If not, remove data from your training data set or obtain licenses or consents where you lack rights. Review whether personal information is being used and, if so, whether that is permitted by existing privacy regulations and privacy policies.

Consider whether synthetic data could be used in lieu of data provided by others or personal information. If not, consider watermarking protected information, such as personal information, in case opt-outs or discovery demands are received.

Supply Chain Governance

Every company will be using an increasing number of AI-enabled tools, and many companies will sell through AI-enabled platforms.

Following the lead of privacy regulations, companies may be responsible for supply chain compliance.

Build your capabilities in contracting for AI-enabled products and services, including how to contract for compliant products, address risk and address the unpredictability of generative and other forms of AI.

In addition, build capabilities in contracting for the critical inputs to your own AI projects, including data, tools and data science talent.

Harm Prevention Before Deployment

Conduct a risk assessment and determine whether the AI presents any risks of harm, such as inaccuracies or bias that would impact credit, health, children or otherwise adversely affect disadvantaged or vulnerable groups.

If so, modify your AI development and deployment processes to mitigate the risks ahead of deployment of the AI. Even after risk mitigation consider adding a nutrition label warning of the remaining possible harms to insulate the company from claims that users were not aware of potential risks, such as a hallucination or bias when they knowingly used the AI.

Ongoing Monitoring

After deployment, conduct bias assessments to determine if protected groups are experiencing greater risks unfair or disparate treatment, especially in the areas of credit lending, housing, employment, education and health care, and if so modify the performance of the AI systems to reduce those risks.

Also, work to monitor the AI to see how it is behaving, and to determine whether risks have been introduced in the algorithms during the iterative process of use of the AI.

Notice to Users

Consider giving clear notice to individuals when they are interacting with AI instead of a person. Notice requirements already exist under S.B. 1001, California's chatbot disclosure law, that went into effect in 2019.[3]

However, notice and transparency are hallmarks of recommendations that came out during the hearing, as well as the various frameworks introduced around the world, including the draft Artificial Intelligence Act in Europe.

Manage IP Rights

Improper monetization by AI companies of content, personal data, artistic works and other creations by citizens may later lead to requirements to pay royalties or even prohibitions on what, absent regulations, could be lucrative businesses.

Board Oversight

Boards, especially in the case of companies where AI assets and/or compliance risks are viewed as mission-critical, should consider at least the following:

- Demonstrating that AI risk is overseen at the board or board committee level and including AI matters as a regular board agenda item that is shown as having been duly considered in board minutes;

- Need for select board member AI expertise or training and/or designated management person with primary AI risk responsibility;

- Relevant directors' familiarity with company-critical AI risks and availability/allocation of resources to address AI risk;

- Regular updates/reports to the board by management of significant AI incidents or investigations; and

- Proper systems to manage and monitor compliance/risk management, including formal and functioning policies and procedures — covering key areas like incident response, whistleblower process and AI-vendor risk — and training.

These steps should help protect directors against claims that could be brought for breach of fiduciary duties under the Caremark case standard, which involved claims of Delaware directors' failure to oversee corporate compliance risks for mission-critical assets even if there had not actually been a regulatory compliance breach.

While bringing Caremark standard cases has traditionally not been easy, recent instances where such claims have survived motions to dismiss highlight the ongoing significance of this claim for directors

responsible for overseeing critical company compliance operations.

Summary

The U.S. appears poised to regulate AI to address growing concern about AI systems, particularly around bias, transparency and privacy.

The hearing suggest future U.S. regulation will lean toward approaches synergistic with frameworks that have been contemplated outside the U.S.

Companies should proactively take stock of these global trends and develop better governance processes now as they build systems, rather than wait for these laws to go into effect. It may be difficult — and expensive — to play catch-up and retroactively document training data and risk mitigation techniques for AI tools once regulation and legislation is in place.

Obviously, prematurely developing systems that are later noncompliant would also be a costly mistake.

The hearing repeatedly emphasized the need to avoid repeating the perceived mistake of not regulating social media. They reflected a desire to take a different approach to AI by adopting early regulation.

More hearings and legislation will follow, including with respect to competition or antitrust concerns, intellectual property, national security and the possible creation of a new AI agency.

Dominique Shelton Leipzig is a partner and leader of the ad tech privacy and data management team at Mayer Brown LLP.

Paul C. de Bernier is partner and global co-leader of the corporate and securities practice at the firm.

Brad Peterson is a partner, the leader of the global technology transactions practice, and the co-leader of the supply chain and distribution practice and the fintech practice at the firm.

Senior counsel James Carlson and special counsel Lawrence Cunningham contributed to this article.

[1] https://www.judiciary.senate.gov/committee-activity/hearings/oversight-of-ai-rules-for-artificial-intelligence.

[2] https://www.judiciary.senate.gov/imo/media/doc/2023-05-16%20-%20Bio%20&%20Testimony%20-%20Altman.pdf.

[3] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.