NACM'S 129TH CREDIT CONGRESS & EXPO Cleveland
MAY 18-21, 2025

AI in the Credit Department: Drafting and Implementing Responsible AI Policies and Procedures

SUPPLEMENTAL MATERIALS/ARTICLES

Presenters: Kathleen A. McGee – Partner, ECVC & White Collar Criminal Defense
Andrew Behlmann – Partner, Bankruptcy & Restructuring Department

Moderator: Bruce S. Nathan – Partner, Bankruptcy & Restructuring Department

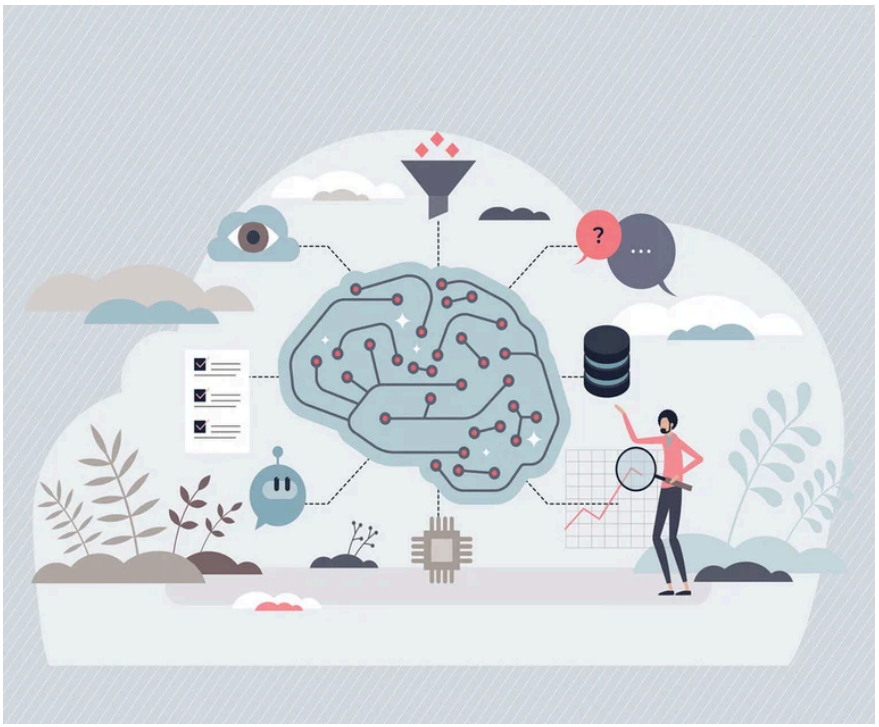
Date: May 21, 2025

Session: # 37064

Lowenstein Sandler

TABLE OF CONTENTS

Legaltech news



An illustration demonstrating artificial intelligence.

COMMENTARY

Does My Company Really Need a Generative AI Policy?

Companies, ranging from creative service firms to hedge funds, are increasingly seeking guidance on implementing generative AI policies that address their unique needs.

December 03, 2024 at 12:57 PM

5 minute read

Artificial Intelligence

By Bryan Sterba
By Mark Kesslen

As generative artificial intelligence (AI) continues to evolve and permeate various sectors, many businesses have started forming and implementing policies to govern its use. These businesses face crucial decisions about how to integrate these tools, including the use of training data and prompts into their operations while managing associated risks. Companies, ranging from creative service firms to hedge funds, are increasingly seeking guidance on implementing generative AI policies that address their unique needs. This brief article explores the diverse concerns and risk profiles of different industries, providing insights into why developing an internally aligned generative AI policy is essential for optimizing usage and minimizing potential pitfalls.

Concerns Across Industries

When consulting with clients across various sectors, we have noted distinct requests for generative AI policies tailored to their specific contexts. Here are three representative types of businesses and their principal concerns:

Creative Service Businesses: These firms often express anxiety about potential copyright infringement when generative AI tools produce materials reminiscent of the content on which the AI tools were trained. The ability of such tools to generate similar—and even identical— written materials or artworks creates a pressing need for policies that safeguard intellectual property rights while still allowing employees to engage in creative ideation with the AI tools. These firms typically seek to identify AI tools that provide broad indemnification rights for infringement caused by the AI tool (offered by many, but frequently subject to caveats and carveouts that leave the customer exposed to significant risk), and develop clear policies for their employees to follow (often opting for simplified “Do and Don’t” lists).

Hedge Funds and Venture Capital: For hedge funds and venture capital funds, the added regulatory scrutiny they face means higher stakes for data security risks and material nonpublic information (MNPI) ingestion when using generative AI. There are heightened risks of inadvertent disclosure of confidential or personal information when using an AI tool that is not locally hosted or on a private instance, or when any MNPI is used to train such AI tools. A generative AI policy for financial services firms must include provisions that ensure adequate cybersecurity measures are in place and restrict the input of confidential information into the AI tools. Venture capital firms may also want to identify a process for ensuring their portfolio companies are using AI tools responsibly as well. In general, policies that include a pathway to new AI tool approval and clear diligence objectives for assessing these vendors are key to empowering employees while setting clear benchmarks for vendors.

Software Solution Businesses: Companies that develop or integrate software solutions look at generative AI as a tool for innovation. However, they must address issues surrounding provenance and

ownership of data used for training and prompts, user data security, infringement risk, open-source license compliance, and the ethical implications of AI-generated solutions. Any drafted policy expected to apply firm-wide must consider each department's concerns—from marketing to product development. As many of these businesses rely on funding from sophisticated investors, (such as the venture capital firms mentioned above) they must stay on the forefront by adopting a policy that addresses responsible usage of AI tools as investors have come to expect such reassurances in funding rounds.

Crafting An Internally Focused Policy

An effective generative AI policy should be internally facing, guiding employees on acceptable usage while considering the diverse needs of various stakeholders. For instance, the creative services sector might allow tools for ideation but prohibit using generative AI to create client deliverables. Conversely, a hedge fund may limit AI tool usage solely to those pre-approved by legal and technology departments based on security assessments and only for specifically approved use-cases. Businesses with preexisting policies addressing aspects of concerns can amend such policies for nuances in AI tool usage, but a more comprehensive approach, with an individual and distinct policy for AI-tool usage that points employees to a single resource, would consolidate the issues and provide more use-case specific guidance.

When formulating a policy, it is critical to ensure practicality. A policy that is too restrictive could inadvertently push employees to circumvent it, rendering the guidance ineffective. To mitigate this risk, organizations should engage their teams in discussions about potential uses for generative AI tools and the data needed to support it. Establishing a framework for employee-driven inquiries into new tools encourages compliance and fosters an environment of accountability.

Legal counsel can assist in identifying the best approach to policy development. Management must ensure that employees clearly understand their expectations, whether they curate a comprehensive long-form policy, a simplistic 'Dos and Don'ts' list, or a hybrid model. Businesses must inform departments subject to specific AI regulations (such as state laws that restrict usage in connection with employment related decision making) of regulations and identify the proper person to contact with questions about implementation.

Conclusion: Tailor Your Approach

Not every business will benefit from a generative AI policy. But no firm will benefit from a policy that is unnecessarily restrictive or does not comply with laws applicable to its business. Organizations must critically assess their needs and risks before adopting any standardized 'one-size-fits-all' policy.

Organizations should also consult with legal counsel to determine if a generative AI policy is necessary and what guardrails to establish. A policy that promotes innovation and creativity without unnecessary

restrictions that stifle initiative can satisfy the optimal goal of empowering employee and increasing efficiency.

A generative AI policy tailored to fit specific business needs enables companies to better navigate the evolving AI landscape, harness the benefits these tools offer, and protect their interests.

Bryan Sterba is a partner in Lowenstein Sandler's emerging companies and venture capital who advises clients on how to leverage emerging technologies to achieve their business objectives and day-to-day intellectual property and commercial contract matters.

Mark Kesslen *is chair of the firm's intellectual property group. He devotes his practice to clients engaged in creating businesses, launching new products, and conducting M&A and venture capital transactions.*

Sage Therapeutics was named in a stockholder derivative complaint on March 26 in New York Southern District Court. The lawsuit, brought by Rigrodsky Law and Grabar Law, takes aim at certain officers and directors for allegedly overstating the efficacy, safety and commercial prospects of its primary drug candidates, includi...

Read More

New Suit – Data Breach Class Action

New York University was hit with a data breach class action on March 26 in New York Southern District Court over a data breach that exposed the personal

Open My Radar

LAW.COM PRO

ALM Market Analysis Report Series: Heightened Competition for Talent is Driving Change in New York City

Am Law 200 Real Estate: Trends and Analysis

The Analyst View: The Legal Market Trends to Navigate in 2025

More from ALM

Legal Speak is a weekly podcast that makes sense of what's happening in the legal industry.

Browse all Products

Legalweek Sneak Peek: The State of AI In the Legal Industry

1 minute read

Legal Speak Spotlight: 'Sidebar With Saul' Revisits Historic Trump Trial And Verdict

1 minute read

Trump v. Big Law: Vivia Chen Believes the Industry Needs to Fight Back

1 minute read

Sign Up Today and Never Miss Another Story

As part of your digital membership, you can sign up for an unlimited number of complimentary newsletters from Law.com by visiting your My Account page and selecting Newsletters to make your selections. Get the timely legal news and analysis you can't afford to miss, curated just for you, in your inbox, every day.

Subscribe to Law.com Newsletters 

February 18, 2025

Top AI Risks General Counsels Should Address

By Diane Moss, Ken Fishkin CISSP, CIPP/US, CIPM, CIPT, and Judith G. Rubin CIPP/US/E, CIPT

Considering the rapid development and deployment of artificial intelligence (AI) in a wide array of applications and business sectors, it can be a daunting task for a company's General Counsel (GC) to keep pace in identifying and managing associated risks. The following overview of the major legal, compliance, and cybersecurity risks is intended to help you understand which AI-related risks a GC may typically face and how to minimize them.

A company will typically be confronted with AI risks in the following contexts, which we will address in more detail below.

1. Identifying and Understanding AI: A tool may contain AI features without the user being aware of it, a vendor may be using AI without the knowledge of its customers, and a company's understanding of the scope or functions of an AI tool may be incorrect.
2. Allowing and Limiting the Use of AI: Employees may be using AI without authorization, and AI tools may be used in a way that exceeds what they were meant or approved for.
3. Data Quality, Rights, and Confidentiality: The quality of the underlying data (including the right to use such data) is of particular importance in the context of AI and machine learning. Moreover, AI tools may not meet confidentiality and privacy requirements.
4. Cybersecurity Risk Management: The use of AI by threat actors can lead to more sophisticated attacks, and integrations with third-party tools can make a company more vulnerable.
5. Evolving Legal and Regulatory Landscape: Laws, regulations, and best practices are still adapting to the new technology, and legal and contractual obligations are not always clear and predictable.
6. Data Governance and Accountability: Lack of clear responsibilities and expectations means that a company will not be sufficiently prepared for the risks associated with the new technology. Regulators, business partners, and customers, on the other hand, are paying more attention to these issues.

1. Identifying and Understanding AI

Companies are always adding new features to their services, but in the case of AI, third parties may be slipping new AI features into their products without notifying users about this fact and the associated risks it might cause. It is thus advisable to carefully vet the vendors of such software, understand the tool's terms of use, and routinely review any feature release notes to identify new or modified AI use cases.

2. Allowing and Limiting the Use of AI

Shadow IT: When employees feel the ability to do their work is hampered by existing policies or tools, they will often develop workarounds to make them more efficient, even though they may be bypassing security protocols. By accessing public AI tools and inputting private or confidential information into them, they could be causing a security breach for the company. Companies should implement a workflow with the procurement department to ensure that due diligence is performed before any tools or services are purchased.

Access Control: Implementing the proper access controls for an AI system is critical for three reasons: security, integrity, and privacy. If access controls are not designed and tested adequately, there is a risk that the data could be accessed by an unauthorized user, which would allow them to either steal the data or tamper with it on purpose or accidentally. Companies should perform regular access reviews to ensure that only the necessary people have access to AI tools, and that their permissions are limited to what is needed to perform their jobs. Too often, employees are given more access than needed.

3. Data Quality, Rights, and Confidentiality

Companies usually use AI tools to boost efficiency, streamline internal workflow processes, or facilitate the provision of services to customers. By deploying tools that were trained on high-quality data, companies can realize these advantages and mitigate the risk of business disruptions, fines, and reputational harm associated with the use of output that is illegal, inaccurate, infringing, or biased. Consider implementing the following best practices:

- Use models trained on accurate, complete, relevant, and representative data.
- Assume that biases will exist, and proactively address any concerns that are relevant to the use case.
- Understand that as potentially helpful as the tool may be with respect to business operations, outputs are only as reliable as the training material and may contain errors or perpetuate biases and discriminatory practices.
- To mitigate these risks:
    - Confirm the source of training data and the vendor's practices to ensure data quality during the diligence process to vet a tool.
    - Seek the inclusion of representations and warranties from the vendor to decrease exposure for inaccuracies and biases.
    - Incorporate the obligation for human review of output to confirm that the material is accurate and reliable as part of your company's responsible AI business practices. Human involvement is critical as machines can make mistakes, even if quality training data was used.

4. Cybersecurity Risk Management

Vendor Management: Performing sufficient due diligence on third parties that offer AI solutions is imperative since a company is responsible for the data it manages. Companies should require that a vendor does not add features that might increase risks without giving adequate notice. At a minimum, ask the following basic questions:

- In what geographic location(s) is the vendor's data stored?
- Can the vendor's data be used for training purposes?
- Does the vendor have adequate cyber insurance?
- Does the vendor have a SOC2 Type 2 report or ISO 27001 certification?
- What third parties does the vendor utilize?

Companies should also consider regularly reviewing existing vendor contracts to ensure that they still meet required cybersecurity and confidentiality obligations.

Employee Training: Most data breaches currently involve the human element. AI has made cyberattacks easier to execute and more convincing than ever. All employees should thus undergo cybersecurity training during their onboarding process and regularly thereafter. Such training should cover potential threats like phishing scams and social engineering tactics, malware protection, how to prevent attacks, and how to handle any security incidents that may occur.

5. Evolving Legal and Regulatory Landscape

Rapid development of laws and lack of harmonization – both globally and within the U.S. – are two of the most challenging aspects of AI regulation. Various parts of the world have adopted varying approaches to AI governance and thus created a patchwork of laws that can be difficult to navigate.

In the U.S., regulation of AI at the federal level has been limited. Several agencies including the CFPB, FTC, and SEC have all issued rules and guidance regarding the use of AI or technologies of which AI is included, and have focused generally on AI adoption that is transparent and conspicuous. Guidance was also issued by the National Institute of Standards and Technology. Much more regulatory progress has been made on the state level, where several states have enacted AI-related legislation, and many more bills have been proposed. The proposed and enacted bills vary widely in scope and obligations. Utah's Artificial Intelligence Policy Act, for example, requires disclosure when using AI tools with customers. California recently enacted two AI laws that will take effect in January 2026 and require developers to be transparent about AI training data and offer AI detection watermarking tools. And the new Colorado AI law, which becomes effective in February 2026, requires developers and deployers of "high-risk artificial intelligence systems" to protect consumers from risks of algorithmic discrimination.

Internationally, countries are approaching AI governance variously via voluntary guidelines and standards, use-specific or comprehensive legislation, and national AI strategies. To mention just a few of these developments: In Europe, the European Union's (EU) Artificial Intelligence Act became effective in August 2024. It has extraterritorial scope and applies to AI systems placed on the EU market or used in the EU by or on behalf of companies located throughout the world. China has adopted multiple laws focusing on the use (as opposed to the development and deployment) of AI. Canada's proposed Artificial Intelligence and Data Act aims to protect Canadians from high-risk systems and ensure the development of responsible AI. Singapore, on the other hand, is taking a sectoral approach and lets the respective authorities publish regulations and guidelines.

While one can observe some common patterns, there is no standard approach to AI regulation, and we can expect that the legal landscape will further evolve as AI technology advances. Businesses are thus advised to stay informed about new developments and be prepared to adapt to new rules.

6. Data Governance and Accountability

Accountability may be the ultimate risk mitigator because being "accountable" requires deployers to be knowledgeable about the multifaceted complexities of AI and encourages cross-teaming with colleagues in different verticals such as privacy, IT, security, and data governance to address its risks.

The prospect of building an effective AI governance program may seem daunting but is not as hard as you think. Even for businesses that do not have the necessary financial and organizational resources to adequately protect their IT infrastructure from common cyber threats or ensure that their AI tools are well protected can implement an AI usage policy as an effective and low-cost way to communicate use restrictions to employees.

Companies that require a robust program can start building such a program by doing the following:

- Identify existing policies, such as confidentiality, privacy, and data compliance policies, that can be leveraged in the context of AI. The principles governing these areas dovetail nicely with the pillars of AI governance (data security, privacy, quality, transparency, contestability, and redress).
- Identify colleagues who have the level of expertise and authority to assess and approve the risk associated with the in-house use of AI tools. Staff members in IT, information security, and privacy can offer valuable assistance in tool diligence and help confirm if tools are safe or appropriate for the respective use case.
- Establish a process and protocol for tool vetting and approval. Along with vendor diligence, make sure your employees know not to download AI applications without prior approval in accordance with the company's established process. To streamline the approval process, it can be helpful to establish a preapproved list of AI tools and associated permitted and prohibited use cases. Applications are not universally acceptable in all use cases and may present larger risks outside the context of the intended use.
- Train your employees in the processes and guidelines. A well-articulated framework is particularly important for its effectiveness. Users must understand the processes and use limitations of applications.
- Establish AI output review protocols to ensure human oversight.

- Establish monitoring and oversight responsibility for the use of AI tools and the laws and regulations that apply to them.
- Work with senior management to establish AI incident response plans and risk management strategies to prepare for situations of misuse or errors related to the use of an AI application.
- Stay current on evolving and emerging AI laws and regulations and related accountability requirements, and maintain an agile framework that is built to adapt.

As a GC of a company that deploys AI tools, AI accountability means that you can answer "yes" to the question "Do we have a defensible AI governance process in place that addresses the tool's life cycle with the company?"

Conclusion

Over the past few years, ChatGPT and other AI tools have taken the world by storm. As a result, GCs must quickly adapt to the changing business landscape and update their AI risk assessments accordingly. Understanding the top AI risk factors, such as access rights, data governance, cybersecurity risk management, data quality management, and the legal and regulatory landscape, is essential to providing GCs with a starting point for developing adequate policies and procedures so their employees can use AI responsibly. Once these policies and procedures are finalized and enforced, GCs should have the necessary guardrails in place to provide their company, clients, and customers with adequate cybersecurity, integrity, and privacy protections.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

DIANE MOSS
Counsel
T: 973.597.2448
dmoss@lowenstein.com

KEN FISHKIN, CISSP, CIPP/US, CIPM, CIPT
Senior Manager of Information Security
T: 973.422.6748
kfishkin@lowenstein.com

JUDITH G. RUBIN CIPP/US/E, CIPT
Counsel
T: 212.419.5908
jrubin@lowenstein.com

Lowenstein AI: A-I Didn't Know That
Video 4 – Do I Need a Generative AI Policy?

By Bryan Sterba

February 4, 2025

Bryan Sterba: Hi, I'm Bryan Sterba, and welcome to another installment of "A-I Didn't Know That."

As artificial intelligence continues to evolve, it is crucial for businesses to establish clear guidelines to ensure its ethical and effective use. Generative AI has become an integral part of many business operations enhancing productivity, improving decision making, and offering innovative solutions. But its use also comes with significant responsibilities and potential risks.

Establishing a comprehensive AI usage policy helps a company to ensure compliance, maintain ethical standards, protect data privacy, and mitigate other risks.

A clear generative AI policy should include several components:

- It should define the policy's purpose and scope of its application, specifying which AI tools are covered and who is authorized to use them.
- It should outline acceptable and unacceptable uses of AI tools.
- It should establish guidelines for handling data, ensuring compliance with data protection laws, and implementing measures to secure sensitive information.
- It should require transparency and documentation in all AI operations. Generative AI policies should clearly outline the implementation process, offer resources and support to employees for AI related queries, and articulate enforcement mechanisms such as regular audits.

It is essential that the company make clear that it will take appropriate action against any violations of the AI policy in order to maintain integrity and trust.

Thank you for watching. Join us next time on "A-I Didn't Know That."