The Elements of a Corporate AI Policy - A Blog Post by Michael Whitener

This is the second in a series of VLP Technology Transactions Group articles on the legal challenges of artificial intelligence (AI).

In a previous blog post in this series, Brian Swanson noted the importance of your organization having a written AI usage policy. This blog post dives into the necessary elements of such a policy.

The arrival of ChatGPT took many (including me) by total surprise. New and even more surprising AI developments will arrive hard and fast. Is your company ready? How do you want to both permit and rein in your workforce in their use of these fascinating and potentially productivity-enhancing new AI tools?

A recent McKinsey Global Survey confirms what McKinsey calls "the explosive growth" of generative AI in the workplace. Yet that same survey found that only 21 percent of the surveyed companies have established policies governing employees' use of AI technologies. As discussed in more detail in our previous blog post in this series, corporate use of AI without policy guardrails is courting disaster.

Guiding principle: every company should have an AI policy. The policy should cover both permitted and forbidden uses of AI for workplace purposes, including the following topics:

1. **Purpose and Scope**

What are the core objectives of the AI policy? To set the tone, the policy should encourage the informed and responsible use of generative AI for purposes of increasing efficiency, improving decision-making and fostering innovation. But the policy should also acknowledge that AI benefits come with potential risks, including data protection breaches, copyright violations, protection of confidential information, ethical considerations and compliance with legal obligations. Thus the policy should aim at maximizing the benefits of generative AI while minimizing the very real risks.

In terms of scope, the policy should apply to any use of generative AI by the organization's workforce (including consultants and contractors as well as employees) for business purposes, whether at the office or remotely. The policy should also dovetail with existing corporate policies, such as a Code of Conduct and Ethics, a Data Protection Policy, an IT and Communications Systems Policy and a Diversity, Equity and Inclusion Policy.

2. **Authorized Generative AI Tools**

The company should consider the approach it wants to take with respect to the scope of permitted generative AI tools. Generally speaking, the company can either (i) list specifically permitted AI tools

and provide a procedure for approval of other tools, or (ii) permit use of any reputable AI tool other than certain listed tools for which use is prohibited (e.g., because of concerns about the security, intellectual property integrity or reliability of the prohibited tools). In either case, the list will need to be updated periodically as new AI tools are introduced and current AI tools are modified or retired.

For an AI tool to be considered "reputable" it should permit the user to opt out of any data entered by the user from being used to train the tool itself (or that may be the default position). If use of the data for training the tool is the default position, the AI policy should require company users to select the opt-out option.

3. **Permitted Uses**

The AI policy should specify the business purposes for which authorized AI applications can be used. Examples of permitted uses could include conducting research, drafting internal memoranda and presentations, producing marketing materials, developing code, summarizing documents and idea generation. For uses not specifically permitted, the policy should provide an established procedure for prior approval.

4. **Guidelines for Use**

The AI policy should describe the company guidelines that any use of generative AI tools must comply with. The guidelines should cover at least the following:

- *Use of company data.* AI prompts must not include any confidential, sensitive or proprietary employer or third-party customer, supplier or employee-related data.
- *Use of personal data.* Personal data, especially sensitive personal data, should not be entered into the AI tool unless truly necessary and subject to all legally required personal notices and consents.
- *Compliance with intellectual property rights.* The user must be aware of and comply with any copyright, database rights and trademark rights of third parties with respect to data entered into the AI tool.
- *Discriminatory language.* The inputting of offensive, discriminatory or otherwise inappropriate content should be forbidden.
- *Security.* The same security standards that apply to all corporate IT applications (including of course third-party applications) should apply to AI tools. The security commitments of the AI tool should be reviewed to ensure compatibility with the company's security measures.
- *Output review.* The risks of "hallucinations" and other inaccurate outputs when using AI tools have been well publicized. Before relying on AI output for any critical purposes, the output should be confirmed with other reliable sources.
- *Ethical guidelines.* The company and its workforce should commit to using AI applications ethically and responsibly. This commitment includes addressing foundational issues such fairness, transparency and minimizing biases in AI outcomes.

5. **Monitoring**

The AI policy should explicitly grant the company the right to monitor all content, including prompts and output, regarding any AI tools used for business purposes. The purposes of such monitoring should be made clear: to prevent misuse of corporate and customer information, to comply with laws regarding intellectual property and personal data rights, etc.

Note that, depending on the AI tool, monitoring may be a challenge, as tools such as ChatGPT host prompt data for only 30 days before deletion.

6. **Training and Technical Support**

The effectiveness of AI tools is contingent on users understanding the tools' capabilities. Regular training ensures employees are informed and can harness AI technology appropriately. The AI policy should describe what training the company makes available and whether the training is mandatory. Any applicable regulatory restrictions (which at this point are mostly just proposals) should be addressed in the training.

Since AI tools are such a new development, your workforce may have challenges in using them along the way. It's recommended that your company have a point person for addressing any technical issues with AI tools.

7. **Breaches of the AI Policy**

As with any corporate policy, the AI policy should spell out how any breaches of the policy will be dealt with, including disciplinary action. Given the potential risks to a corporate enterprise of using generative AI as a workplace tool, sanctions for misuse are not only appropriate but necessary.

The policy should also require (i) cooperation with any investigation into a suspected breach of the AI policy and (ii) reporting of any AI policy breaches.

* * *

VLP Law Group: Your Partner in Navigating the AI Landscape

Navigating the confluence of generative AI tools and corporate use of these tools requires a partner with both technological acumen and legal expertise. VLP stands at this intersection, staffed with a dedicated team of legal professionals attuned to the challenges and opportunities of AI.

Let's collaboratively chart a course for a future where your business thrives in an AI-augmented landscape.