The Importance of Establishing a Policy on the Use of AI Within Your Organization - A Blog Post by Brian Swanson

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

Artificial intelligence, and in particular large language models and generative AI, has burst into the public consciousness, and appears by all accounts to be a transformative technology in today's digital age. While AI has been around longer than you might think, the recent release of Open AI's ChatGPT tool and the broad availability of other generative AI tools has caused an explosion of interest and focus on artificial intelligence, and in the use of such tools.

These generative AI tools are here to stay, and it is very likely that many of your employees and contractors have already incorporated these AI tools into their workflows for tasks ranging from coding to content creation and data analysis. The potential benefits that use of these generative AI tools can bring to your organization are vast. Yet, it is imperative to understand and manage the inherent risks by taking proactive measures, such as establishing and implementing an AI usage policy, before those risks result in damage to your enterprise.

Some of the key risks associated with use of generative AI tools in the workplace are the following:

Privacy Violations. Use of personal information about customers, employees or others that your enterprise may possess is subject to applicable privacy laws and privacy policies. Even if the intended use is legally permissible, it may require you to revise your privacy policy, obtain the consent of the affected individual, or take other actions before that use is permissible, if at all. If your employee or contractor uses that information in an AI tool before a thorough review of the intended use, the AI tool itself and the applicable laws and policies has taken place, it can result in significant liability to your organization.

Inaccuracy and Reputational Risk. While generative AI tools are trained on a vast amount of data, there are still gaps in that data, and not all of that data is accurate. In addition, AI tools have been known to "hallucinate", i.e. to make up information in response to a request. In one well-publicized cautionary tale in the legal field, an attorney used an AI tool to assist in preparing a legal brief, only to discover after submitting the brief that the output from the AI tool included references to cases that did not exist. If your employees or contractors rely on an AI tool for information and use it in an important work context a process in place for fact-checking that information, your organization could suffer similar reputational and other damage.

Bias and Discrimination. AI tools are a reflection of their training data, and as a result can perpetuate existing biases. This can be particularly problematic in the employment context. If an AI tool is used by someone in your organization in making an employment decision without adequate consideration of the potential bias, it could give rise to a claim of discrimination. In addition, a number of U.S. states and cities are implementing laws requiring disclosure or consent or imposing other restrictions on the use of AI in certain employment contexts, which if ignored could result in legal liability for your organization.

Ambiguity in Ownership of Output. The terms and conditions under which AI tools are made available vary widely, and not all of them grant ownership or rights to use their output for any purpose. For example, they may not permit commercial use of their output. And even if the terms of the AI tool grant you the rights you need, the vendor of the AI tool may not have the authority to grant you those rights. Many AI tools are trained on vast quantities of data and content without the consent of the owners of that data or content, and the rights of AI tool owners in that output is the subject of current litigation the final outcome of which is unclear. Additionally, your employee or contractor may have signed up to use an AI tool in their individual capacity, restricting any use of the output to them in their individual capacity and not by you on behalf of your enterprise. It is critical to consider these issues before output of an AI tool is used by your organization, to avoid taking on unwarranted liability or suffering other significant business consequences (for example most acquirers of software companies will conduct a thorough review of ownership of the software code of a target, and a messy ownership situation may well kill a potential deal).

Lack of Copyright Protection. The U.S. Copyright Office takes the position that content generated by AI tools is not eligible for copyright protection, since it was not authored by a human. This position, although currently being contested in court, means that even if the AI tool provider's terms grant you ownership to its output, you may find yourself unable to prevent competitors or others from copying and using as they see fit, software, logos or other critical assets of your enterprise that were generated through the use of AI tools.

Loss of Trade Secret Status. Trade secret protection for your critical confidential information relies on your enterprise taking reasonable steps to preserve its confidential status. However, many AI tools use user inputs to train the AI model. If you permit your employees or contractors to submit source code or other critical confidential data or information of your enterprise to such an AI tool, that data or information could lose its trade secret status on the grounds that you have not taken reasonable steps to protect it.

Infringement Concerns. Large language models are trained on large amounts of content, often without the consent of those who might have ownership or rights to that content and arguably infringing or violating their rights. In addition, the output generated by AI tools could be considered a derivative work of underlying content used in the model, infringing the copyright of the owner of the original content. These issues are currently being litigated in a number of cases against the creators of prominent large language models, and the ultimate outcome is unclear. Although recently some AI tool vendors, including Microsoft and Adobe, have announced plans to provide IP indemnification coverage to customers relating to the use of certain of their paid AI tools, at present the terms and conditions for most AI tools do NOT provide you with any recourse or protection if their training or output infringes or violates third party rights. If you get caught up in a related lawsuit, you will need to bear the costs of defending that suit and paying any resulting judgment, with little or no ability to seek

compensation from the AI tool vendor.

Breach of Contract. Use of AI tools by your employees or contractors can give rise to additional contractual risks. For example, your employee could input information or data of your customer into an AI tool without considering contracts you have with that customer. If your contract with that customer does not permit that use of their information or data, you could suffer significant liability for breach of contract in addition to having an unhappy customer (or former customer).

Despite the many risks associated with use of AI tools, thoughtful use of AI tools within your organization can bring incredible benefits and may well be necessary in order for you to compete in the business landscape of the future. But in order to reap those benefits in a manner that limits the associated risks, it is critical for you to establish a written company AI usage policy. Your AI policy should be a living document, which provides for periodic reviews and updates to ensure that the policy keeps pace with the rapid evolution of AI and with the use and anticipated use of AI tools within your organization. The policy must cover all aspects of the use of those AI tools and should be created with the input and consideration of all groups within your organization. Once your AI policy is established, the policy should be shared broadly within the organization and accompanied by appropriate guidance and training to insure its successful implementation.