Best Practices for Mitigating Intellectual Property Risks in Generative AI Use

Mai Tong Yang

Published 01/15/2025

Generative AI (GenAI) is transforming the business landscape, unlocking new possibilities for innovation, productivity, and efficiency. As with any major shift, GenAI comes with its own risks, particularly in intellectual property (IP) and legal compliance which organizations must navigate to fully capitalize on its potential.

What You Need to Know:

- **Clarify IP Ownership:** Document human contributions and establish clear agreements with AI tool developers, model providers, and other parties to define ownership and intellectual property rights.
- **Minimize Infringement Risks:** Implement processes to review AI outputs, enforce compliance with copyright and trademark laws, and prevent unauthorized use of third-party content.
- **Safeguard Sensitive Data:** Protect trade secrets and proprietary information with strict security protocols and review AI platform terms to prevent confidentiality breaches.
- **Ensure AI Governance and Compliance:** Develop internal AI policies, conduct thorough vendor due diligence, and regularly update policies to address evolving legal and regulatory requirements.

Clarifying IP Ownership for AI-Generated Works

When it comes to AI-generated content, determining ownership can be complex and requires careful attention to detail. While there has been some guidance from the U.S. Patent and Trademark Office and the U.S. Copyright Office, there is still uncertainty around how much human involvement is needed for these works to be eligible for copyright or patent protection. To protect your IP interests, it is important to document human contributions to any AI-assisted projects and make sure you have clear agreements in place with all parties involved—such as model providers, AI tool developers, and end users—so that ownership and IP rights are well-defined.

Minimize IP Infringement Risks

Using GenAI can put your business at risk of copyright infringement, both due to the data used in training AI models and the content it generates. For instance, AI models may be trained on datasets containing copyrighted material without proper authorization, and the outputs may unintentionally mirror or closely resemble protected works. To manage these risks, your business should: (1) create a process for reviewing and clearing AI outputs, and (2) implement clear policies that ensure compliance with copyright and trademark laws, preventing unauthorized use of third-party content.

Safeguard Trade Secrets and Proprietary Information

Your business must be diligent in protecting sensitive business information when using AI platforms, as these platforms often require user input to generate outputs. Without appropriate safeguards, there is a risk of inadvertently disclosing proprietary data. Additionally, certain platform terms of service may grant providers rights to use or retain input data, potentially compromising confidentiality. To mitigate these risks, your business should implement comprehensive security protocols and ensure strict oversight of confidential information to protect your interests.

Opt for Enterprise AI Licenses

Choosing enterprise-grade licenses can establish robust protections. These licenses often offer clearer terms regarding IP ownership, enhanced security measures, and specific provisions for warranties, indemnification, and confidentiality. Given the complexities of AI-related agreements, organizations should carefully review these terms and ensure that all parties—such as AI tool developers and service providers—have clearly defined roles, so that data, outputs, and legal rights are properly safeguarded.

Conduct AI Vendor Due Diligence and AI Assessment Procedures

Implementing a thorough due diligence process when selecting AI vendors is essential for ensuring security and compliance. This process should include using tailored questionnaires to assess the vendor's security measures, IP ownership terms, and alignment with the organization's legal and operational requirements. By carefully evaluating these factors, risks can be mitigated and ensure AI partnerships are well-managed and secure.

Establish an Internal AI Policy

A robust internal AI policy is essential for mitigating IP and legal risks while ensuring effective AI governance. The policy should mandate rigorous testing and validation of AI tools before company-wide deployment. To oversee implementation and ensure comprehensive risk management, a cross-functional team of legal, compliance, and IT professionals should be formed. Critically as important, providing ongoing training for employees is crucial to ensuring compliance with AI usage guidelines, IP protections, and data security protocols, thereby safeguarding IP interests.

Monitor and Adapt Policies as Needed

As the legal and regulatory framework for GenAI continues to evolve, your business must remain vigilant in monitoring these changes. Regularly updating internal policies to ensure compliance with emerging laws, address new risks, protect IP rights while capitalizing on advancements in AI technology.

If you have questions about these best practices or need assistance in developing your company's AI-related policies, please contact Leah Leyendecker or a member of the Saul Ewing AI Group.

Author

Mai Tong Yang

Associate

(612) 225-2616 | ✉

View bio

Related Services

Artificial Intelligence (AI)

Intellectual Property