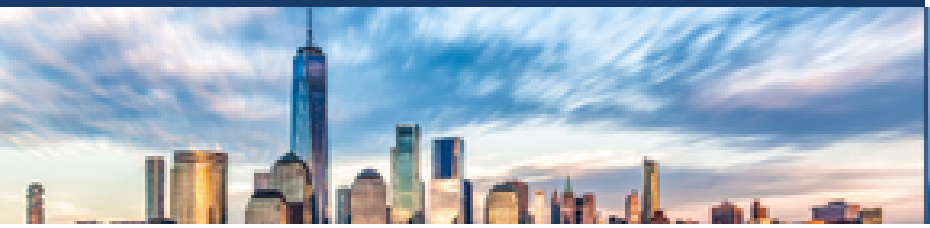
By: Russell H. Stern, Esq. and Alexandra C. McCormack, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.




Legal Considerations for Businesses in the Age of Artificial Intelligence

The rapid adoption of artificial intelligence ("AI") technologies is transforming how businesses operate. As a firm, Ruskin Moscou Faltischek P.C. has observed numerous instances where AI is being leveraged effectively by our client base. However, we have also encountered just as many instances where AI's deployment in the business setting has introduced complex legal and operational risks, resulting in heightened liability for the company's principals and equity holders.

Across industries, we are seeing an uptick in employment-related decisions being made with the assistance of AI, which presents legal and ethical concerns. Further, professionals in the healthcare and veterinary sectors are employing AI for diagnostics, treatment recommendations, and patient monitoring, which raises a host of regulatory and data privacy questions that must be carefully managed. A few of the industry-agnostic AI issues, along with suggested steps to best protect your business, are highlighted below.

Protection of Confidential Information and Trade Secrets

The sharing of sensitive company-specific information with AI platforms by employees or contractors of a business can inadvertently expose proprietary knowledge to the outside world, unless proper precautions are taken. Companies need to determine if they will be using an open or closed AI platform, or a combination of both. To mitigate risk, companies should implement internal training on permissible AI use and consult with counsel to draft company-specific policies. Further, companies should review existing third-party agreements and confidentiality arrangements to ensure that company data and trade secrets shared externally are protected.

Intellectual Property and Ownership

AI-generated works raise questions regarding intellectual property ownership and use rights. Businesses must carefully evaluate whether they own or have the legal right to use AI outputs, especially when relying on third-party AI platforms, such as ChatGPT. Failure to obtain proper licenses, or to negotiate contractual intellectual property rights could expose a company to future claims of infringement.

Data Privacy Concerns

Companies handling personal identifiable information (PII) and other sensitive information, especially those in the health and financial sectors, must proceed with caution when integrating AI into their business practices. Companies must ensure compliance with applicable data privacy laws, including the federal Health Insurance Portability and Accountability Act (HIPAA), New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD) and the California Consumer Privacy Act (CCPA), among others. Businesses should proactively implement data management protocols (internal and external) and conduct regular audits of AI usage. Failure to properly manage PII and AI use may result in regulatory enforcement actions, civil and/or criminal liability and reputational damage.

Regulatory Compliance and Liability Exposure

Companies may face legal liability for AI-driven decisions, particularly in areas such as employment, lending, healthcare, and other highly regulated sectors. Businesses should establish compliance frameworks and internal policies that address errors and potential biases to avoid violating the law.

Recommendations for Proactive Risk Management

1. Conduct a risk assessment before allowing company personnel to engage with AI technologies.
2. Determine whether a closed or open AI platform will be used, or a combination of the two, and what the policies and rules are with respect to either or both.
3. Review and implement internal contractor and/or employment policies with respect to AI use and reduce to writing.
4. Review and update contracts and licensing agreements with third-party providers to clarify use, rights and responsibilities with respect to proprietary and otherwise confidential information of the company.
5. Review AI processes and output for veracity and to ensure biases are not being inadvertently introduced into company decision-making.
6. Redact documents of any and all sensitive data before uploading or sharing with AI technologies and require the same of third-party service providers.
7. Monitor legislation, regulatory guidance, and industry best practices to ensure ongoing compliance with evolving legal requirements.

For more information on how to best protect your business in the age of AI, please contact:

Russell H. Stern, Esq.
516.663.6582
rstern@rmfpc.com

Alexandra C. McCormack, Esq.
516.663.6653
amccormack@rmfpc.com