Strategic Foundations for Ethical and Legally Compliant AI Adoption in Legal Sector: What Lawyers Need to Know before Using AI Professionally.

By: Karl V. Hopkins
Bradley
600 Travis, Suite 5600
Houston, TX 77002

Emily Westridge Black
Sherman & Sterling
800 Capitol, Suite 2200
Houston, TX 77002

Artificial Intelligence (AI) is a disruptor in multiple industries, offering transformative solutions that redefine traditional processes. The legal industry, characterized by its stringent regulations and complex ethical considerations, is now at a crossroads with AI's emergence. The increasing sophistication of machine learning algorithms and natural language processing capabilities offers unmatched opportunities but poses complex legal challenges. Similarly, the integration of AI into legal practices is not without its complexities, given the rigorous regulatory environment and intricate ethical dilemmas that characterize the field. Similar to their clients, lawyers need to be aware of and comply with the relevant AI regulations in their jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, or the proposed Artificial Intelligence Act (AIA) in the EU, seeking to regulate data protection, data privacy and the ethical use of AI

As machine learning algorithms and natural language processing capabilities continue to advance, they present unprecedented opportunities and complex challenges for legal practitioners. An Oxford University report shows that AI can improve and simplify legal tasks like reviewing documents, analyzing contracts, researching laws, or supporting litigation. However, AI-assisted lawtech poses risks such as data security, ethical quandaries, and interpretive errors.

Two foundational elements are instrumental for lawyers and their clients seeking to harness the advantages of AI responsibly: a robust, internally articulated AI governance policy and a carefully negotiated Master Service Agreement (MSA) with AI vendors. The former is an indispensable guidepost, aligning the firm’s AI initiatives with prevailing legal norms, ethical mandates, and strategic objectives. This internal policy demystifies AI functions, delineates accountability, and institutes transparent procedures for secure and ethical data management. For instance, an AI governance policy could specify how you or your clients will ensure data quality, privacy, and security when using AI for document review or contract analysis. It could also define how you will monitor and audit the performance and accuracy of AI tools when using them for legal research or litigation support. Simultaneously, the MSA establishes a critical framework for the external relationship between your practice, or your clients, and the AI service provider. It outlines provisions concerning data ownership, utilization rights, and confidentiality safeguards, thereby serving as a bulwark against potential breaches, misinterpretations, and other legal or operational pitfalls by controlling ownership over your information and work products and clarifying how the

vendor will ensure compliance with applicable laws and regulations, including the confidentiality of your clients' information.

In essence, the mastery of AI governance and MSA negotiation isn't merely a skill set that enriches your own practice; it places you in an invaluable advisory role for your clients as well. Navigating the complexities of AI adoption in a legal context, therefore, is not an option but a necessity for modern legal professionals, both for their own operational integrity and as trusted advisors to their clients. Consequently, this article aims to delve into the intricacies of establishing a robust AI governance policy and negotiating a comprehensive Master Service Agreement (MSA) with AI vendors. By scrutinizing these foundational elements, the article seeks to equip legal practitioners with the requisite knowledge and tools to navigate the ethical, legal, and operational complexities inherent in adopting AI technologies

I. Understanding the Elements of AI Governance Policies []

For legal practitioners, AI governance is an indispensable framework to adeptly traverse the multifaceted and evolving challenges posed by AI ethics and legal norms. Such governance equips attorneys with the necessary tools to deploy AI technologies in a manner that is congruent with ethical principles, professional values, and strategic objectives while also aligning with the expectations of clients, regulatory bodies, and societal norms. Moreover, a strong AI governance protocol offers a safeguard against the manifold risks associated with AI, such as inherent biases, computational errors, security vulnerabilities, potential liabilities, and ethical conflicts. Thus, in the legal profession, crafting a comprehensive AI policy has transitioned from being a subject of futurology to a strategic necessity.

1. The Objectives of an Effective AI Policy

    a. Ethical Use and Legal Compliance

A good AI policy serves as a guide through the complex issues of AI ethics and law. The policy needs to be carefully designed to guard against biases, ensure accountability, and uphold principles of fairness. In the context of legal landscapes that are constantly evolving, the policy helps maintain legal compliance, reducing legal and reputational risks. This includes alignment with data protection norms, privacy laws, and intellectual property rights. Transparency and accountability, therefore, serve as the cornerstones of a policy aimed at ensuring ethical and legally compliant algorithms that respect the confidentiality of client data.

As to legal practices, AI policy is a vital tool to navigate complex and dynamic issues as it helps legal practitioners to design, deploy, and use AI systems in a way that is consistent with their values, principles, and goals, as well as the expectations and interests of their clients, regulators, and society. It also helps your practice to mitigate the potential harms or risks of AI systems, such as biases, errors, breaches, liabilities, or conflicts.

    b. Risk Management and Operational Efficiency

A key goal of an AI policy for lawyers is to balance innovation with risk effectively. This balance depends on the technology's strengths and the organization's ability to handle risks. At its core, a comprehensive AI policy optimizes operational efficiency while adhering to the highest legal

compliance standards and ethical responsibility. This article will elaborate on how risk management and operational efficiency are intricately linked in an AI policy and why striking the right balance between them is imperative.

i. Role Clarity and Operational Efficiency

Roles and responsibilities must be clearly defined for an AI policy to work efficiently. Unclear roles can cause mistakes and delays, leading to serious legal and ethical problems. An organization ensures a smooth workflow by explicitly outlining who is accountable for what in the AI system's lifecycle—from deployment to maintenance to oversight.

An attorney who uses AI systems in their practice must be aware of their roles and responsibilities, as well as those of other parties involved, such as the AI developers, providers, users, and regulators. For example, an attorney needs to know who is responsible for the quality, accuracy, reliability, and security of the AI system, who is liable for any damages or harms caused by the AI system, and who has the authority to access, modify, or delete the data or outputs of the AI system.

ii. Privacy and Security Risks

In the age of data breaches and increasing concerns about individual privacy, any AI policy must include rigorous privacy and security protocols. Given that AI systems often require access to large sets of data, including potentially sensitive or personally identifiable information, the risks of unauthorized access or data leakage are significant.

Attorneys are bound by ethical and legal obligations to protect the confidentiality and integrity of client information. Any breach or unauthorized access to this sensitive data can result in severe legal consequences, including potential disbarment and civil or criminal liability. Given that AI systems often process and store vast amounts of data, some of which may include privileged client information, ensuring robust security measures is critical. Thus, an effective AI policy should set strict data encryption, access control, and auditing standards. It should also mandate regular security audits and include contingency plans for potential breaches. Addressing these privacy and security risks proactively meets legal compliance standards and builds trust with stakeholders, thereby promoting operational efficiency.

iii. Financial Considerations

While AI systems promise significant efficiencies and capabilities, they come with direct and indirect costs. Financial risks might include deployment costs, ongoing maintenance, and potential legal liabilities. An operative AI policy will require a rigorous cost-benefit analysis that evaluates the economic viability of AI adoption against these potential risks. Such an analysis can inform budget allocations, guide resource optimization, and set realistic expectations regarding return on investment (ROI), contributing to overall financial efficiency.

A lawyer should be well-versed in the economic dimensions of AI adoption for a variety of reasons, each of which carries considerable weight in terms of both ethical responsibilities and practical necessities. An understanding of the financial risks and requirements associated with AI is essential for the fiduciary responsibilities lawyers owe to their clients and, in some cases, shareholders or partners within a firm. Implementing AI can incur significant costs, including

Title search: Practical Considerations and Implications of Generative AI

Also available as part of the eCourse
First Friday Ethics (April 2024)

First appeared as part of the conference materials for the
2023 Essential Cybersecurity Law session
"Practical Considerations and Implications of Generative AI"