ALM | LAW.COM
LAW JOURNAL NEWSLETTERS

CYBERSECURITY LAW & STRATEGY

# Empowering Legal Professionals: Navigating AI Solutions for Efficiency and Data Security

BY MICHAEL T. MURRAY AND TONY DONOFRIO

APRIL 2024

The emergence of artificial intelligence as a viable tool in the practice of law promises both efficiency and elevated enterprise risk. Integrating AI tools into legal practice without compromising the security of sensitive client information is a paramount concern. In this article, we'll examine how AI is revolutionizing certain aspects of legal work, while offering best practices for employing these technologies and providing guidance for legal professionals in selecting the right AI products and service providers.

## The Intersection of AI and Legal Practice

The integration of AI in the legal sector is transforming the landscape of legal practice, introducing unprecedented efficiencies in case management, document review and legal research. Zach Warren, manager of technology and innovation at the Thomson Reuters Institute, encapsulates this transformation succinctly: "Legal generative AI is **supposed to augment** what a lawyer does. It is not going to do legal reasoning, not going to do case strategy. What it's supposed to do is do repeatable rote tasks much more quickly and efficiently." This shift allows legal professionals to focus on the substantive aspects of their work, ensuring higher-quality outcomes and more effective client service. However, to effectively unlock this potential without introducing material liability and reputational risk, stringent data protection and governance measures are required. Following is a brief rundown of processes where AI will be of value, along with information privacy and risk management considerations for each use case.

### *Faster Data Analysis and Routine Document Synthesis*

In the daily grind of legal practice, generating, reviewing and distributing standard-form content, such as contracts and filing motions, can be streamlined using AI. Generative AI, coupled with expert human oversight, significantly reduces the production time and effort while improving quality in the production of such content. The efficiency is generated by the speed drafting, while quality is improved by having a second set of AI "eyeballs" on final draft, providing comparison and comments against other similar content.

Using AI in this way requires particular attention to the following risks:

- Work product and copyright compliance. Content generated by large language models may contain content published and copyrighted in publicly available form, such as journals and other news media. Lawyer review of any generated content should include considerations for appropriate citation references where applicable.
- Content bias. Both generation and analysis of content using AI models are subject to societal and cultural biases based on the particular model's source content exposure. Review of analysis, and of generated content, must bear this in mind.

### *Efficient Legal Research*

Generative AI technologies offer a substantial advantage in legal research by jump-starting the process, reducing the hours or even days traditionally spent sifting through and summarizing content. This not only saves time but also allows lawyers to apply their expertise to refine the results, ensuring that the research output is thorough, accurate and of high quality. Zena Applebaum, global VP of product marketing for research products at Thomson Reuters, highlights the efficiency of this technology: "For any of the tasks that lawyers do on a regular basis, this technology allows them to do those things faster and create a starting point much earlier in the process."

Using AI in this way requires particular attention to data privacy and security risks. When applying client or firm data to query, or especially train, an AI model, ensuring the data is not permanently stored or available in any way for public use is critical.

### *Navigating Complexity with Plain-Language Prompting*

Generative AI tools capable of understanding plain-language queries significantly lower the barrier to searching and accessing content. Think about the power of "asking a set of documents a question" versus "searching for an indexed word." This advancement allows for quicker, more effective development of arguments and strategies by rapidly organizing relevant information and precedents.

Using AI in this way requires particular attention to the following risks:

- Data privacy and security (as noted above)
- Content bias (as noted above)
- Quality degradation. As with humans, AI answers are particularly variable based on how the questions are posed. Ensuring concept searches are both comprehensive and accurate will be important to guarantee high-quality analytics.

The security and privacy of legal data are paramount. Professional, licensed generative AI tools offer a secure ecosystem for working with proprietary data, minimizing the risk associated with public-facing tools. Moreover, as these tools are trained on high-quality legal content, they promise outputs that are both trustworthy and accurate, distinguishing them from other large language models.

## Vetting AI Vendors: Key Considerations

The widespread use of AI, from unlocking our phones to predicting our next favorite movie, underlines its potential to streamline business procedures in legal services. However, the selection process for AI vendors involves critical considerations beyond just technological capabilities.

When selecting an AI vendor, it is critical to ensure an alignment with your firm's legal and ethical standards as well as data security requirements. A vendor's flexibility, not just in terms of tools, but also in legal services like videography and real-time transcription, is crucial. The balance between embracing rapid technological advancements and maintaining accuracy and reliability is delicate.

Transparency is a cornerstone of a trustworthy AI vendor relationship. Legal professionals should inquire whether AI tools are used as assistive content or are considered final products. The consensus is clear: AI-generated material should not be regarded as the final work product; you need a skilled professional behind the machine. Even the most technologically advanced solutions rely on trained, professional reporters to capture and manage the preservation of the record and certify accuracy.

Beyond that, the security of derived content and the proprietary nature of AI models are critical factors. Vendors should not only protect confidential information but also ensure their AI models are built on secure, private content, preventing any inadvertent sharing through systemwide training models.

What are the critical factors for vetting AI vendors?

### *Legal Environment Alignment*

With AI laws in place across various jurisdictions, understanding the legal landscape is vital. The procurement process must consider data privacy, disclosures and cross-border transfers, adjusting the evaluation criteria to ensure compliance with specific legal regimes.

### *Risk Assessment*

The deployment of AI introduces risks of bias, fairness, transparency and environmental impact. This underscores the importance of making sure you are collaborating with a partner you can trust to help navigate these complexities while providing the security needed to keep your data and organization safe.

### *Data Privacy and Processing*

In jurisdictions with stringent privacy laws, thorough disclosures regarding data collection and processing are necessary. Vendors must demonstrate transparent practices and robust data protection measures to ensure compliance and protect consumer rights.

### *Vendor Compatibility*

Beyond the technical fit, assessing a vendor's commitment to privacy, transparency and ethical standards is key. This involves scrutinizing data handling practices, compliance with privacy laws and the transparency of the AI algorithms.

### *Collaborative Vetting*

The responsibility for vetting AI extends beyond in-house counsel to include IT, security teams, legal and compliance departments, data protection officers and external counsel. This collaborative effort ensures a comprehensive evaluation from technical, legal, ethical and business perspectives.

By incorporating these expanded considerations into the vendor vetting process, legal professionals can navigate the AI landscape with a more informed and holistic approach. This ensures not only the efficient integration of AI into legal services but also adherence to ethical standards and regulatory compliance, safeguarding the interests of clients and the organization.

### Aligning AI Procurement with Legal and Ethical Standards

AI's application extends into critical areas like cybersecurity, health care, finance and legal services, underscoring its potential to enhance efficiency. Yet this comes with inherent responsibilities, especially in legal environments where privacy, data ethics and compliance with evolving regulations must be maintained.

The responsibility for vetting AI solutions often falls to general counsel, sometimes late in the procurement process. This necessitates a nuanced approach that evaluates AI not only for its immediate benefits but also for its long-term implications on privacy, ethics and regulation. The "**Brussels effect**" and similar regulatory frameworks globally demand that organizations align their AI strategies with legal requirements, making compliance a critical factor in vendor selection.

### Testimonial Evidence Management and AI Automated Speech Recognition

While AI offers remarkable efficiencies in various domains, its role in legal transcription remains a topic of debate. Although AI excels in areas like predictive analytics and big data, it often falls short in meeting the high accuracy demands when taking the record of testimonial evidence. The nuanced and complex nature of language, as well as the broad variability in audio capture, requires a level of precision that AI speech recognition simply cannot deliver consistently.

Understanding the purpose of AI in legal proceedings takes a shift in thinking. AI-generated materials should not be considered the final product but rather raw, inadmissible initial drafts that can be useful for boosting efficiencies and working on tasks that don't require an accurate record more quickly. AI-generated materials should not be confused with any certified transcript, videography or other material. Certified capture is the role and responsibility of the officiating reporter as the ultimate guardian of the record.

Utilizing the ways that AI technologies can complement the work of skilled reporting professionals is the happy medium. AI can help legal professionals work quickly and efficiently when draft materials or a head start on a project is needed. When selecting which AI tool to use, factors such as accuracy, security and the provision of an officer of the court to capture the certified record should be considered.

As legal professionals navigate the evolving interface of AI and legal practice, insights from industry leaders provide invaluable guidance. By carefully selecting AI solutions that prioritize efficiency without compromising data security, legal practitioners can harness the benefits of technology while upholding their commitment to client confidentiality and ethical practice. The key is making sure to balance the best of the efficiencies and speed of AI technologies for draft inadmissible materials with the skilled reporting capture of the certified record by the officer of the court. Here are key points to consider when using AI-based products and services in your discovery and management of testimonial evidence:

- Careful use of "raw" AI-generated text and audio/video content. Content produced from sources such as a remote deposition recording, augmented with AI analysis or summarization, can be effective for rapid review and strategy, but should never be construed as replacing a human-reviewed official version with certified accuracy assessed by an unbiased professional.
- Content security/chain of custody. Content produced by your service providers, as well as your firm's staff, should be vetted to ensure that your data is protected at rest and in transit and is never inappropriately utilized by the plethora of third-party tools and platforms proliferating rapidly in the marketplace.

*****

**Michael T. Murray** is the director of client solutions for Veritext Legal Solutions. Murray stays on top of litigation technology trends and travels throughout the nation speaking and providing informative and entertaining CLEs, educational instruction and product demonstrations to legal professionals.

**Tony Donofrio** is the chief technology officer at Veritext. He develops and supports the mission-critical systems clients, reporters and employees use every day. His focus at Veritext is to ensure that clients and Veritext staff have the very best experience with easy-to-use, highly reliable and highly secure tools.