



2024 International Client Seminar

February 29 - March 3, 2024

Artificial Intelligence – The New Gold Standard

Tamara K. Nelson

Co-Moderator

MERRICK HOFSTEDT & LINDSEY, P.S.

Seattle, WA

tnelson@mhlseattle.com

Paul G. Klockenbrink

GENTRY LOCKE

Roanoke, VA

klockenbrink@gentrylocke.com

Artificial Intelligence in Business and Law

What is AI?

AI refers to the simulation of human intelligence processes and the ability of machines to solve problems. It involves computers' capacity to interpret intricate data, identify patterns, and make decisions – a task previously exclusive to humans. Significantly, these algorithms can learn over time, addressing challenges across various business domains.

AI technology is transforming the way data, information and knowledge are processed, facilitating new interaction environments. The application of artificial intelligence in the enterprise is profoundly changing the way businesses work.ⁱ Companies are incorporating AI technologies into their business operations with the aim of saving money, boosting efficiency, generating insights, and creating new markets.ⁱⁱ There are AI-powered enterprise applications to enhance customer service, maximize sales, sharpen cybersecurity, optimize supply chains, free up workers from mundane tasks, improve existing products and point the way to new products.ⁱⁱⁱ

The application of artificial intelligence to the legal sector has consequences (1) modernization of the working methods and (2) practice and assessment of the consequences of the new services in different sectors.^{iv} AI offers jurists various tools that are useful to carry out the work, allow prediction of outcomes in the legal proceedings and also allow a massive analysis of documents and identification of patterns.

What can AI do? ^v

Process Automation:

AI is playing a pivotal role in transforming process automation by leveraging machine learning and robotic process automation (RPA) technologies. AI-driven automation optimizes workflows, reduces manual tasks, and enhances overall operational efficiency. This innovation allows businesses to analyze extensive datasets, make data-informed decisions, and automate repetitive processes, leading to accelerated operations. Industries ranging from manufacturing to customer service benefit from AI's ability to streamline tasks, enabling human resources to focus on more complex aspects of their roles. AI in process automation is a powerful tool for organizations seeking increased efficiency, agility, and innovation in their day-to-day operations. AI has proved to be an effective tool for automating time-consuming processes that are often prone to human error. By automating processes, organizations can free up employees to work on more complex projects. Some of the key benefits of AI include (and by way of example, the preceding paragraph was generated with the assistance of ChatGPT):

Increased Efficiency: AI streamlines repetitive tasks, ensuring they're done faster and with fewer errors. In inventory management and supply chain automation solutions, it optimizes order processing, reducing lead times.

Cost Reduction: Automating tasks means fewer labor hours and lower operational costs. AI helps in inventory management by reducing excess stock and minimizing storage costs.

Enhanced Decision-Making: AI analyzes vast amounts of data, providing insights humans might

overlook. Supply chain automation helps in real-time decision-making by considering multiple factors like demand, transportation, and supplier performance.

Scalability and Consistency: As your business grows, AI scales effortlessly without compromising quality. For inventory management, it ensures a consistent approach to managing inventory levels across multiple locations.

Improved Supplier Relationships: AI can assess supplier performance and suggest the best suppliers based on historical data, leading to cost savings and better relationships within the supply chain.

Inventory Accuracy: AI ensures precise tracking and reduces the chances of discrepancies between actual inventory and what's recorded in the system. This accuracy is crucial for inventory management, preventing stockouts and overstock situations.

Adaptability to Market Changes: AI quickly adapts to changing market dynamics, allowing businesses to respond to fluctuations in demand, supplier availability, or market trends. In inventory management, this adaptability ensures that your stock aligns with customer needs and market shifts.

Financial reporting and accounting:

AI-powered systems can generate financial reports automatically based on predefined templates and formats. These systems can extract relevant data, perform calculations, apply accounting rules, and produce comprehensive reports without human intervention.

Automating financial report generation offers numerous benefits to businesses. Firstly, it significantly reduces the time and effort required to compile and create reports, enabling finance teams to allocate their resources to more strategic and value-added activities.

Secondly, automation minimizes the risk of human errors and inconsistencies by extracting data directly from financial systems, ensuring accuracy and reliability in the reports.

Additionally, automated report generation allows for increased agility and flexibility, as reports can be generated on-demand or scheduled to run at specific intervals, providing real-time insights for decision-making. This streamlined process enhances overall efficiency, improves data integrity, and empowers organizations to make informed financial decisions in a timely manner.

Automation of financial report generation can bring scalability benefits to businesses. As organizations grow and generate increasing amounts of financial data, manual report generation processes become arduous and time-consuming.

IT Operations Management:

AI is extensively utilized in the IT industry for various applications, including but not limited to automated system monitoring, predictive maintenance, cybersecurity, IT service desk automation, data management, network optimization, compliance monitoring, talent acquisition, and disaster recovery planning.^{vi} With the ability of AI to determine repetitive patterns, this process can be run easier and faster. Using AI for data analysis allows QA departments to eliminate human errors, reduce running test time, and easily identify possible defects. AI application in IT is widespread, including:

Automated Incident Detection and Resolution: AI employs machine learning algorithms to

monitor IT systems continuously. It can swiftly identify anomalies, irregularities, or potential security threats in real-time, enabling a proactive response to incidents. Automated incident resolution, driven by AI, reduces downtime, minimizes manual intervention, and fortifies the organization's cybersecurity posture.

Predictive Analytics for Performance Optimization: Leveraging historical and real-time data, AI enables predictive analytics to forecast potential performance issues and bottlenecks. By identifying patterns and trends, IT operations can proactively address potential problems before they impact system performance, ensuring optimal functionality and preventing service disruptions.

Capacity Planning and Resource Allocation: AI plays a pivotal role in optimizing resource utilization through intelligent capacity planning. By analyzing data on resource usage patterns, AI helps IT teams make informed decisions about resource allocation, ensuring that infrastructure scales seamlessly with demand while minimizing costs.

Automated Root Cause Analysis: When incidents occur, AI-driven root cause analysis swiftly identifies the underlying issues. This accelerates the troubleshooting process, reducing downtime and allowing IT teams to address the root causes promptly, leading to more resilient and reliable IT operations.

Chatbots for IT Support: AI-powered chatbots provide instant IT support, offering solutions to common issues and answering queries. This not only enhances user experience but also reduces the burden on IT help desks, allowing them to focus on more complex issues while routine queries are handled efficiently by AI-driven virtual assistants.

Configuration Management Automation: AI streamlines configuration management by automating routine tasks related to system configurations. This ensures that IT environments remain consistent, compliant, and secure, mitigating the risks associated with configuration errors and enhancing overall operational stability.

Automated Patch Management: AI automates the process of identifying, testing, and deploying software patches. This not only enhances security by promptly addressing vulnerabilities but also ensures that systems are running the latest versions of software, optimizing performance and stability.

Continuous Monitoring and Optimization: AI enables continuous monitoring of IT environments, providing real-time insights into system performance, security, and resource usage. This continuous feedback loop allows IT operations teams to optimize configurations, make data-driven decisions, and adapt to changing conditions promptly.

Uptime/Reliability Optimization:

The integration of AI in uptime and reliability optimization is reshaping how businesses maintain and enhance the performance of their systems and processes. AI technologies, such as predictive analytics and machine learning, are employed to analyze data patterns, detect anomalies, and forecast potential issues before they lead to downtime. By harnessing AI's ability to process vast amounts of data in real-time, organizations can proactively address maintenance needs, minimize equipment failures, and optimize overall system reliability. This proactive approach not only reduces downtime but also enhances operational efficiency and extends the lifespan of critical assets. AI in uptime/reliability optimization is becoming a cornerstone in industries such as manufacturing, energy, and

telecommunications, empowering businesses to achieve higher levels of reliability and operational continuity.

For companies that rely on web services or e-commerce, maintaining uptime and website reliability is a top priority. AI helps organizations achieve this by constantly scanning systems, networks, and processes for inefficiencies, potential disruptions, and to identify any looming threats in a way humans could never accomplish. For companies that offer round-the-clock digital services, using AI can help identify problems before they start, while also reducing instances of crashing, hacking, and human error.

Cybersecurity:

Artificial Intelligence (AI) is revolutionizing the field of cybersecurity, providing advanced capabilities to detect, prevent, and respond to cyber threats. AI algorithms, including machine learning and deep learning, are employed to analyze vast datasets and identify patterns indicative of potential security breaches. This proactive approach enables real-time threat detection and response, bolstering defenses against evolving cyber threats. AI-driven cybersecurity systems can autonomously adapt to new attack vectors, improving their ability to recognize and mitigate sophisticated threats. From anomaly detection to behavioral analysis, AI enhances the overall resilience of cybersecurity measures, safeguarding sensitive data and protecting organizations from cyber-attacks with greater efficiency and effectiveness. As cyber threats continue to evolve, the integration of AI in cybersecurity is crucial for organizations seeking robust and adaptive defense mechanisms. A few examples of artificial intelligence cybersecurity include:

Threat Detection and Anomaly Identification: AI algorithms are adept at analyzing vast datasets in real-time to identify patterns indicative of potential security threats. By continuously monitoring network traffic, user behavior, and system logs, AI-driven systems can swiftly detect anomalies and suspicious activities, enabling proactive threat mitigation.

Behavioral Analysis and User Anomaly Detection: AI employs behavioral analysis to establish a baseline for normal user activities. Deviations from this baseline trigger alerts, signaling potential unauthorized access or compromised accounts. This proactive approach enhances the ability to detect insider threats and sophisticated attacks that may evade traditional rule-based systems.

Predictive Analysis for Advanced Persistent Threats (APTs): AI's predictive analytics capabilities allow organizations to anticipate and defend against Advanced Persistent Threats (APTs). By analyzing historical data and identifying patterns indicative of APTs, AI provides insights to fortify defenses and mitigate the impact of prolonged and stealthy cyber-attacks.

Autonomous Incident Response: In the event of a security incident, AI-powered systems can autonomously respond by isolating compromised systems, limiting the spread of malware, and initiating remediation processes. This swift response time is crucial in minimizing the damage caused by cyber-attacks and reducing the overall impact on organizational operations.

Phishing Detection and Email Security: AI enhances email security by identifying and blocking phishing attempts in real-time. Machine learning models analyze email content, sender behavior, and other contextual factors to identify suspicious emails, preventing employees from falling victim to phishing scams and social engineering attacks.

Endpoint Security and Threat Hunting: AI-driven endpoint security solutions provide real-time protection by analyzing the behavior of endpoints and detecting malicious activities. Threat hunting capabilities enable security teams to proactively search for and neutralize potential threats before they escalate.

Adaptive Authentication: AI contributes to adaptive authentication systems by continuously evaluating user behavior and adjusting authentication requirements accordingly. This enhances security by adding layers of protection based on the risk level associated with specific user activities.

Vulnerability Management and Patching: AI streamlines vulnerability management by prioritizing and automating the patching process. By analyzing the risk associated with different vulnerabilities and assessing the organization's overall security posture, AI helps ensure that critical vulnerabilities are addressed promptly.

Security Information and Event Management (SIEM): AI enhances SIEM systems by automating the analysis of security events and logs. This not only accelerates threat detection but also allows security teams to focus on investigating and responding to high-priority incidents.

Human Resources:

Leveraging AI throughout the employee lifecycle—including for sourcing and recruiting candidates, onboarding, managing employee records, and developing existing team members—can help human resources teams drive efficiencies and keep talent engaged.^{vii} Some of the many use cases for AI in human resources include:^{viii}

Writing content for recruitment materials: Recruitment and talent acquisition teams can use generative AI tools such as ChatGPT or Google Bard to help draft copy for recruitment purposes, including job descriptions, interview questions, candidate outreach emails, and job offer letters.

Automating candidate screening: AI technology can automatically screen candidates based on specific criteria and qualifications and weed out individuals who aren't a fit. These systems often include capabilities to send automated emails to candidates letting them know they aren't moving forward. This enables recruitment and talent acquisition teams to focus their time on the most qualified talent.

Driving candidate engagement: Similar to customer service chatbots, some employers are embracing chatbots as an innovative solution to drive candidate engagement. Companies include AI chatbots and virtual assistants on their career pages to direct individuals to jobs that align with their skills and experience, guide them through an interactive application process, and answer common questions along the way.

Simplifying workforce planning: Talent management systems and human resources information systems centralize employee data, making it easier for companies to manage and automate HR processes. Through these systems, organizations can manage payroll, benefits, time, and attendance, learning and talent development, and other HR functions. Many of these systems also include data related to talent reviews, performance, engagement, retention, and skills, helping organizations better understand worker competencies, skills gaps, and future workforce needs.

Honing focused data for employee evaluations: Succeeding in employee recognition involves being able to provide specific feedback for employees, pinpointing their good work, and highlighting the

areas that need improvement. With AI technology, HR professionals can gain access to highly specialized data about employee performance, allowing for more focused recognition strategies. Companies that adopt AI tools and software can see key details about each employee's productivity and performance. Tying this data into rewards and recognition programs can ensure that employees receive hyper-focused feedback to truly optimize performance moving forward.

Real-time recognition: AI-driven systems can track and help in recognizing employee achievements in real time. Whether it's meeting a sales target, completing a project, or achieving a personal milestone, AI ensures that timely recognition is provided. Real-time recognition improves immediate feedback, encouraging employees to continue their high-performance efforts.

Predictive analytics: AI can use predictive analytics to anticipate recognition opportunities. By analyzing historical data and patterns, AI can identify when an employee is likely to reach a significant milestone or achieve a goal. This allows for proactive recognition, often before the employee even realizes they've accomplished something noteworthy.

Safety and Quality:

Artificial intelligence in health and safety can revolutionize occupational health and safety by improving the identification of hazards, predicting potential risks, providing real-time monitoring, recognizing unsafe behaviors, detecting unsafe conditions, and suggesting ways to mitigate potential risks.

AI algorithms can predict accidents based on non-compliance, alerting management of potential hazards before they turn into accidents. This can help prevent accidents from occurring, minimizing the risk to workers. Artificial intelligence can play a significant role in occupational health and safety in the following ways:^{ix}

Human Error Reduction: Human errors are the main reason why workers experience injuries at the workplace. Moreover, one tiny mistake can not only put others at risk, but it can also lead to downtimes that can cost millions of dollars. Most workplace injuries happen due to worker fatigue or stress.

Automation of Dangerous Tasks: AI takes over production robots and makes them more efficient. AI can take over all robotic production and use automation to complete the most dangerous tasks in hazardous environments otherwise lethal to humans. Robots have been used to inspect dangerous situations for decades. They can enter hazardous environments and send reports back to a human located in a safe place.

Equipment Control/Predictive Maintenance: Faulty machines and tools are one of the main reasons for personal injuries in the workplace. AI can help identify machines and production elements that are not working properly and propose the best solutions before a disaster happens.

Crime Detection and Prevention: AI can quickly identify suspicious behavior and send alerts in real-time. AI can create automatic triggers that will activate lights and sirens to discourage criminal activity.

Incident Management: When an incident starts unfolding, safety leaders and managers need to be able to contain it in the most effective way possible to minimize damage. AI-based systems can send

alerts and notifications as well as recommend the most effective way to respond to the emergency to achieve the goal.

Incident Investigation: Once the incident has been contained, the next step is to investigate the causes. AI-based systems can aid safety leaders in analyzing data to identify the root cause, severity, and frequency of such an event recurring.

Identification of hazards/Predicting Risks: AI can be used to analyze large amounts of data from a variety of sources, including incident reports, safety observations, and sensor data, to identify potential hazards. This can help organizations identify and address hazards before they cause accidents or injuries. AI can be used to predict the likelihood of accidents and injuries occurring based on historical data and other factors. This can help organizations develop and implement preventive measures.

Detecting Behaviors: AI can improve occupational health and safety by predicting workers' unsafe behaviors based on their safety performance. By analyzing data from previous accidents, near-misses, and non-compliances, AI algorithms can identify patterns of unsafe behavior in workers. AI cameras can detect changes in body position, gestures, working style, normal and abnormal movements, and habits to monitor worker behavior, including observing safety protocols.

Real-time monitoring and alerting: AI systems can monitor worker activity if an employee is at risk, engaging in unsafe acts, taking shortcuts, making non-compliance, not wearing PPE etc. AI can generate real-time alerts for supervisors and workers to stay within the safety protocols. AI-powered CCTV or video surveillance systems can be used to monitor workers and workplaces for unsafe conditions and behaviors. This can help organizations to identify and address potential problems before they lead to accidents or injuries.

Training and education: AI can develop and deliver customized training and education programs based on various health and safety topics and emergency scenarios. AI can then suggest future controls, such as providing specific training to improve safety performance or modifying the work environment to reduce risk factors. The system can provide a list of personalized recommendations based on the worker's past performance, ensuring that the worker receives the most effective training. By providing workers with personalized recommendations, AI can encourage workers to take greater responsibility for their safety and help them develop a safety-focused and safety-first mindset. This can also improve the overall safety culture within the workplace.

Workforce Schedule Optimization:

AI is helping companies streamline efforts that once took up a lot of time for managers. AI has helped companies optimize scheduling, considering several factors such as employee availability, customer traffic, and employee skillsets and preferences, all at once to identify the optimum schedule. Leveraging machine learning algorithms and predictive analytics, AI systems analyze historical data, employee performance metrics, and external factors to generate optimized schedules that align with business goals and employee preferences. These systems consider variables such as peak demand periods, employee skill sets, and regulatory compliance, ensuring a well-balanced and compliant workforce schedule. By automating this intricate process, AI not only minimizes the risk of human error but also allows for real-time adjustments based on changing conditions. Workforce schedule optimization powered by AI not only enhances productivity but also promotes employee satisfaction by

creating schedules that align with individual preferences and work-life balance, contributing to a more agile and harmonious workplace environment. (The preceding paragraphs was generated with the assistance of ChatGPT).

Customer Service Operations:

Customer care is the number one priority for any business. It works as a way of customer retention and, if done right, can convey a sense of professionalism and outstanding approach, which build brand integrity. AI can help transform how businesses engage with customers, identify relevant insights, and improve the customer experience. Common applications of AI in customer service include:

Chatbots and Virtual Assistants: AI-powered chatbots provide instant responses to customer queries, offering a seamless and immediate support experience. These virtual assistants leverage natural language processing (NLP) to understand and respond to customer inquiries, handling routine tasks and providing 24/7 assistance.

Automated Ticketing Systems: AI streamlines the handling of customer support tickets by automatically categorizing and prioritizing them. This ensures that critical issues receive prompt attention, improving resolution times and customer satisfaction.

Personalized Customer Interactions: AI analyzes customer data to personalize interactions, offering tailored recommendations, promotions, and responses. This enhances the overall customer experience by making interactions more relevant and engaging.

Voice Assistants: Integrating AI-powered voice assistants into customer service operations enables users to interact with systems using natural language. This is particularly valuable in call centers, as it allows for hands-free communication and efficient issue resolution.

Predictive Analytics for Issue Resolution: AI analyzes historical customer data to predict potential issues or trends, enabling businesses to proactively address concerns before they escalate. This predictive approach minimizes service disruptions and ensures a more proactive and customer-centric approach.

Sentiment Analysis: AI tools analyze customer feedback, social media mentions, and other communication channels to gauge sentiment. This provides valuable insights into customer satisfaction levels and allows companies to address concerns or trends in real-time.

Self-Service Portals: AI-driven self-service portals empower customers to find solutions to common issues independently. Virtual assistants guide users through troubleshooting processes, reducing the need for human intervention and enhancing the customer's sense of control.

Fraud Detection: AI algorithms are employed to detect and prevent fraudulent activities, securing customer transactions and protecting sensitive information. This helps build trust with customers and ensures the integrity of financial transactions.

Language Translation: AI-powered language translation facilitates seamless communication with customers from diverse linguistic backgrounds, breaking down language barriers and expanding the reach of customer service teams.

Customer Journey Analysis: AI analyzes customer interactions across various touchpoints to gain

insights into their journey. This understanding allows businesses to optimize processes, identify pain points, and deliver a more cohesive and satisfying customer experience.

Marketing:

Artificial intelligence tools and machine learning algorithms are used by marketing teams to analyze data, identify customer trends and patterns, optimize marketing campaigns and strategies, and enhance the customer experience. In addition to improving marketing strategy results, AI can also help employees save time by automating manual tasks. Here are several key applications of AI in marketing:

Customer Segmentation and Targeting: AI analyzes vast amounts of customer data to identify patterns and preferences, enabling more precise segmentation. This allows marketers to tailor their campaigns to specific audience segments, delivering personalized content and offers that resonate with individual preferences.

Predictive Analytics: AI-driven predictive analytics uses historical data to forecast future trends and behaviors. Marketers can leverage this capability to anticipate customer needs, optimize campaign strategies, and allocate resources more effectively.

Personalized Content Recommendations: AI algorithms analyze customer behavior to provide personalized content recommendations. Whether on e-commerce platforms, streaming services, or social media, AI helps deliver relevant content to users, increasing engagement and conversion rates.

Marketing Automation: AI automates repetitive marketing tasks, such as email campaigns, social media posts, and ad placements. This not only saves time but also ensures timely and consistent communication with the target audience.

Ad Targeting and Optimization: AI analyzes user behavior and engagement patterns to optimize ad targeting. This includes programmatic advertising, where AI algorithms automate the buying of ads in real-time, ensuring that ads are shown to the most relevant audiences.

Voice Search Optimization: With the rise of voice-activated devices, AI is crucial in optimizing content for voice search. Marketers need to adapt their strategies to cater to the unique characteristics of voice searches, and AI helps in understanding and responding to these queries effectively.

Social Media Monitoring: AI tools monitor social media platforms to analyze brand mentions, sentiment, and trends. This information provides valuable insights for adjusting marketing strategies, managing brand reputation, and engaging with customers on social channels.

Dynamic Pricing: AI enables dynamic pricing strategies by analyzing market conditions, competitor pricing, and customer behavior. This helps businesses set optimal prices in real-time, maximizing revenue and staying competitive.

Content Creation: AI tools assist in content creation by generating written or visual content based on user preferences, trends, and data analysis. This can include personalized product recommendations, blog posts, or social media content.

Legal Departments:

Corporate legal departments process and analyze large volumes of data and documents. Rather than reviewing documents and completing other administrative processes manually, AI can simplify

many legal tasks, enabling lawyers to spend more time providing clients with expert guidance. Here are some specific ways that AI can be used in legal departments:

Research and analysis: Legal research involves spending a significant amount of time reviewing legal cases, laws, regulations, and precedents, among other information. AI-powered tools can automatically retrieve, organize, and analyze relevant legal documents, making it easier for legal professionals to find critical information, extract key insights, and make informed decisions.

Contract review and due diligence: Manually reviewing legal contracts and documents can be time-consuming and prone to human error. In addition to being reviewed by human legal experts, AI tools with machine learning capabilities can review and analyze contract language to flag potential issues or unfavorable terms that may otherwise be overlooked.

Document automation: AI can help generate initial drafts of standard legal documents, such as contracts, nondisclosure agreements (NDAs), wills, and leases, saving legal teams time and reducing human error. Keep in mind, while AI can create drafted legal documents, thorough review by a legal professional is critical before using any AI-generated documents.

Compliance: Different industries and businesses have to maintain compliance with specific regulations, such as HIPAA for U.S. healthcare data and GDPR for businesses that collect data from European Union Citizens. Compliance standards are complex and failing to maintain compliance can lead to breaches or penalties. Companies can leverage and train AI algorithms to understand specific laws and regulations and identify discrepancies more efficiently than manual methods.

E-Discovery and Litigation Support: AI can sift through massive volumes of electronic data to identify relevant information for legal proceedings. Machine learning algorithms can categorize and prioritize documents based on relevance, significantly reducing the time and cost associated with the discovery process.

Legal Analytics for Decision Support: AI facilitates data-driven decision-making in legal departments by providing analytics on case outcomes, legal trends, and litigation strategies. Predictive analytics models can forecast the potential success of legal actions, enabling attorneys to develop more informed strategies and allocate resources effectively.

The legal challenges of AI^x

AI brings about several legal challenges, ranging from the question of who should be held accountable for the harm caused by the AI system to concerns about bias and discrimination.^{xi}

Compliance with regulations: AI development and use aren't standardized or strictly regulated. Governments and other regulatory bodies are still determining the scope of the legal framework. However, there are some regulations that are related to AI, such as privacy and data protection laws.

Open-source license compliance: Imagine a scenario where generative AI utilizes open-source libraries and integrates that code into products. This situation can potentially breach Open Source Software (OSS) licenses like GPL, causing legal issues for the organization. For instance, if a company uses ChatGPT to create code for a software product, and the source of the GPT training data is uncertain, there's a risk of violating terms in open-source licenses linked to that code. Doing so could

lead to legal complications, including allegations of license infringement and the possibility of legal action from the open-source community.

Data and privacy protection: AI systems often collect and store personal data, which can raise privacy concerns. Laws such as the General Data Protection Regulation (GDPR) in the European Union regulate data collection, storage, and use by companies.

Bias and discrimination: AI systems are created by humans and are trained on the data they provide. Therefore, if the data is human-generated and reflects societal biases and discrimination, the system will likely replicate and amplify the same mindset. AI models have to be taught not to discriminate based on attributes such as race, gender, or ethnicity.

Liability: As artificial intelligence systems become increasingly autonomous, determining responsibility for any harm they do becomes a tricky legal issue. While the logical answer may be the system creator, the reality is far from straightforward.

Intellectual property: AI technology often involves complex algorithms and software; AI startups have to be aware of the following challenges: ownership of intellectual property created by AI, patents for inventions made by AI, copyright of the AI-generated content, infringement of intellectual property when AI is trained on copyrighted content.

Insurance: Associations must secure suitable insurance to address liability claims in these legal realms. Traditional nonprofit D&O liability and commercial general liability policies may be inadequate. Exploring errors and omissions in liability/media liability insurance is crucial to filling coverage gaps.

Bankruptcy: Pursuant to the U.S. Bankruptcy Code, a debtor in bankruptcy is entitled to assume, assign, or reject executory contracts (subject to court approval). IP licenses, including AI licenses, are typically considered executory contracts as both the licensor and the licensee generally maintain significant ongoing obligations under the agreement's terms.

Antitrust: AI is used by many businesses to engage in potentially anticompetitive behavior in violation of applicable law. For example, AI could be used to facilitate price-fixing arrangements with other AI systems. Furthermore, AI systems in and of themselves could potentially enter into anticompetitive agreements if they are used to test market conditions and conclude that collusion would be a successful means of maximizing profits.

AI Data Protection Best Practices

It is important to make sure that AI-related initiatives are carried out in an ethical and responsible manner, protecting user privacy, data, and fairness. Without understanding and following best practices, one is more likely to face risks of ethical concerns, legal issues, and damage to reputation.^{xii}

Choose the Right AI Tools for Your Needs:^{xiii}

Identify your business needs: Clearly define the specific problems or tasks you want to address and determine which areas of your business could benefit from AI.

Set clear goals: Set measurable goals that align with your business objectives.

Research available AI tools: Explore the market and identify the AI tools that align with your business needs and goals. Consider factors such as functionality, features, scalability, ease of integration, and compatibility with existing systems.

Evaluate the tool's capabilities: Look for factors such as the tool's accuracy, performance, flexibility, customization options, user-friendliness, and the availability of training and support.

Consider data requirements: Assess whether the tool requires a large dataset, real-time data, or specific data formats. Assess necessary data infrastructure to support the tool's requirements.

Assess security and privacy: Consider the security and privacy implications of using the AI tool; such as data handling practices, encryption methods, and compliance with regulations.

Consider scalability and integration: Determine if the AI tool can scale with your business growth. Assess whether it can seamlessly integrate with your existing infrastructure, software, or platforms.

Evaluate cost and ROI: Consider the cost of acquiring, implementing, and maintaining the AI tool. Evaluate the potential return on investment (ROI) by estimating the benefits it can bring to your business.

Conduct a pilot test: Before committing to a particular AI tool, consider conducting a pilot test or proof-of-concept project.

Vendor support and future development: Assess the reputation and reliability of the AI tool's vendor. Consider factors such as their experience, customer support, ongoing development, and their vision for future updates and enhancements.

Strengthen Security Measures: Businesses need to implement robust security measures to safeguard their data and infrastructure from potential harm. AI systems can be vulnerable to attacks and misused for harm. Implementation of strong security measures can create a shield of protection around company assets. Regular security audits and encryption techniques should be employed.

Strict Access Controls: One of the best ways to prevent accidental data exposure is to limit data access to only team members who need to see it. In doing so, organizations prevent unauthorized members from sharing sensitive data in AI training models.

Secure Data Protection Methods: There are many stages in the data life cycle—including ingestion, analytics, sharing and storage—and each requires specific protection methods. Determining when data must be masked, tokenized, or encrypted will help ensure its protection regardless of use.

Data Scrutinization: The more data you input into a generative AI platform; the more likely sensitive data is to fall through the cracks. As such, minimize the amount of data being shared.

Consistent AI Data Protection Training: The aforementioned team should develop training standards for protecting data before, during and after AI projects. That training should be continuously updated to reflect new compliance regulations, threats, and emerging technology trends.

Review and Fact Check Content: AI tools may misunderstand context or even rely on unreliable or biased sources. It is important to double-check the facts and take a look at reliable sources before continuing usage.

Avoid Plagiarism and Copyright Infringement: AI language models like ChatGPT are built using text input and rely heavily on previous data to generate responses. As AI language models process vast amounts of text data, they may unintentionally reproduce content that resembles existing works. Avoid plagiarism and copyright infringement by running AI generated content through plagiarism and AI detection tools or conduct internal checks to verify its uniqueness.

Understand the limitations of AI: AI has its own set of limitations, including lack of context, common sense, creativity, and emotion. AI models heavily rely on patterns found in training data, which may sometimes hinder their ability to fully grasp the intricacies of the real world. Organizations should actively develop strategies to address their limitations while embracing their potential to enhance lives. By striking this balance, they can make the most of AI's capabilities while upholding ethical standards.

Encourage Continuous Learning: Continuous learning programs and AI technology training courses give your team the chance to stay in sync with the latest AI practices, concepts, and techniques.

Monitor and Mitigate Bias: Implement robust monitoring mechanisms and techniques to detect and address biases.

Adopt AI Company Policies: All companies should be proactive in developing AI use policies which balance their employees' use of AI to innovate and streamline while limiting legal risk. A sample law firm policy is included below:

POLICY ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE

I. Overview of Policy

Generative artificial intelligence (“AI”) describes algorithms that can be used to create new content, including audio, code, images, text, simulations, and videos (we refer to AI-created content as “**Outputs**”). This policy is designed to protect attorneys, staff, and clients by promoting AI use in accordance with the law, our professional obligations and ethics rules, and the firm’s standards and commitment to producing high quality work product. **All attorneys and staff must comply with this policy when utilizing generative AI services and tools available to the wider public, such as the ubiquitous “ChatGPT”** (we refer to these internet-based publicly-available AI services as “**Public AI**”). This policy does not govern the use of AI services and tools developed and sold by private vendors with which the Company has signed agreements (i.e., AI tools that might be integrated with Lexis or Westlaw), on a trial basis or otherwise, and has approved such vendors’ security and data governance policies and procedures (“**Private AI**”).

II. Purpose

While the Firm believes there will be benefits as well as risks associated with the future use of AI in representing clients, this technology has not yet been tailored for use in a law firm environment – for example, by accounting for cyber security and data privacy risks – and, therefore, further research and testing is necessary before it is appropriate for attorneys and staff to use AI in direct connection with client work. Consistent with that determination we have an AI Taskforce reviewing different platforms to determine how AI technology might be used by the Firm in the future. We have also adopted this policy to insure compliance with ethical responsibilities and the Firm’s contractual obligations to safeguard client

confidential information; to safeguard the Firm’s confidential and proprietary information; and to comply with data security and data privacy laws.

III. Public AI Policy Resources

A. Attorney and Staff Use of Public AI

In general, Public AI may **not** be used for any work product to be **directly** provided to a client. Any advice or work product produced with the assistance of Outputs from Public AI must be subject to a thorough and meaningful review and verification process to ensure accuracy and completeness, and to ensure that Outputs from Public AI are used in a responsible, legal, and ethical manner.

- Attorneys and staff may **not** use Outputs from Public AI exclusively to draft or otherwise provide legal advice or legal research directly to clients. **Just as you would with Google or other research tools, you must verify and confirm the accuracy of information.**
- If attorneys or staff use Outputs from Public AI to draft any court submission or otherwise in connection with legal proceedings, or to draft or otherwise provide legal advice or legal research as part of a client matter (e.g., to draft an internal memorandum on an issue of law), attorneys and staff are responsible for informing the partner or senior attorney responsible for the matter—who are required to know the scope and extent of the Outputs from Public AI that were used to draft or otherwise provide the legal advice or legal research rendered. To facilitate the responsible attorney’s review, attorneys and staff should highlight or otherwise indicate in the document (using a “Comment” bubble) which provisions were written or developed using the Outputs from Public AI. And the responsible attorney is required to independently verify the accuracy of the Output used.
 - This might include using Public AI to produce an Output that states a general proposition of law (i.e., “a binding contract requires consideration,” coupled with a source identified by Public AI).
 - This might also include using Public AI to produce an Output that helps the attorney formulate, or provides an example of, a contract provision (i.e., a non-compete clause).

B. Inputs to Public AI

Public AI services may take a license to, or ownership over, any text, content, audio, code, images, or other information, provided by you in order to render Outputs (we refer to any information provided to AI in order to receive Outputs as “Inputs”). Know that your Inputs may be extracted, reviewed, used, or distributed by Public AI services. **Accordingly, when using Public AI, confidential information must never be used as an Input, or otherwise, in connection with Public AI.**

- Inputs must not include work product, or templates including, but not limited to, excerpts from work product or templates.
 - This would include the use of a prior brief or contract. For example, copying an excerpt of a brief that includes citations to Second Circuit caselaw, using that excerpt as an Input, and

-
- asking Public AI to generate an Output that replaces the citations to Second Circuit caselaw with citations to Fourth Circuit caselaw.
- This would also include using a prior contract, or contract provision, as an Input to Public AI.
 - Assume that any intellectual property of the firm and its attorneys enters the public domain when it is used as an Input to Public AI.
- Inputs must be entirely generated by the attorney or staff member, and must not contain any third-party content including, but not limited to, the name of a client, the name of any individual, the name of any entity (e.g., a hospital, city, or institution), extracts from client emails, hornbooks, treatises, manuals, etc. If you copy and paste third-party content into Public AI, you could be liable for copyright infringement or theft.
 - Each and every Input must be kept and documented in any Public AI-assisted work product—for instance, where Outputs from Public AI were used in the creation of an internal memorandum on an issue of law.
 - Strictly prohibited Inputs include, but are not limited to:
 - a client’s name, any information that could identify the client, or any confidential or proprietary information;
 - information from a client or third party that is protected by a confidentiality agreement or court order;
 - the firm’s name or the firm’s confidential or proprietary information; or
 - personally identifiable information (“PII”) that directly identifies any individual, such as name, address, social security number, telephone number, email address, or the like.

The firm’s attorneys and staff are individually responsible for the use of Inputs and Outputs and should be prepared to justify their decisions and actions in relation to Inputs and Outputs.

IV. A Statement on Private AI

Public AI services such as ChatGPT, Microsoft Bing and Google’s Bard are for the most part inappropriate for use in legal practice and are subject to the rules and guidelines set forth above. On the other hand, private, legally-focused tools including Casetext’s Co-Counsel, CSDisco, Lexis+ AI, and Henchman’s contract drafting tool are far better suited for law firms because they utilize known data sources, protect confidentiality, and focus on data security.

V. Questions about this policy or the use of AI

The evolution of AI is moving at a mach pace. The Firm recognizes that this policy will need to be updated as AI takes on a larger role, both in our business and the practice of law. AI is like any other technology tool – it has potential for great benefit but has potential for security or ethical violations if not handled properly. The Firm will continue to work with vendors and will update this policy as necessary. However, should anyone have questions regarding this policy or the use of AI while working on Firm matters or on behalf of Firm clients, those questions should be directed to a member of the AI Taskforce. To the extent

necessary, those questions or concerns will be taken up by the Executive Committee and a response will be provided. Consistency is the key, and the Firm recognizes this is a fluid situation that will require everyone to be educated and patient as this technology evolves.

ⁱ Beth Kempton, *How Is AI Used in Business? 10 Ways It can Help*, UPWORK (Aug. 11, 2023), <https://www.upwork.com/resources/how-is-ai-used-in-business>

ⁱⁱ Gary Kuznetsov, *Artificial Intelligence In Business: Benefits, Impact & 5 Industry Examples*, DIGITALSILK (Dec. 18, 2024), <https://www.digitalsilk.com/digital-trends/artificial-intelligence-in-business/>

ⁱⁱⁱ Josh Howarth, *9 Top Business Trends (2024 & 2025)*, EXPLODING TOPIC (Nov. 9, 2023), <https://explodingtopics.com/blog/business-trends>

^{iv} Veta T. Richardson, *Why Corporate Legal Departments Should Lean Into AI*, FORBES (Dec. 19, 2023), <https://www.forbes.com/sites/forbesbooksauthors/2023/12/19/why-corporate-legal-departments-should-lean-into-ai/?sh=70fa47da3005>

^v Mary Pratt, *15 Top applications of artificial intelligence in business*, TECH TARGET (Jun. 21, 2023), <https://www.techtarget.com/searchenterpriseai/tip/9-top-applications-of-artificial-intelligence-in-business>

^{vi} Rakesh Reddy, *6 Major AI Use Cases in IT operations*, ACUVATE (Dec. 14, 2020), <https://acuvate.com/blog/ai-use-in-it-operations/>

^{vii} John Kell, *HR leaders on how AI is changing recruiting and talent management*, FORTUNE (Jan. 12, 2024), <https://fortune.com/2024/01/12/ai-playbook-c-suite-hr/>

^{viii} Tushneem Dhamagadda, *Harnessing The Power Of AI In Human Resources*, HUBENGAGE (Aug. 25, 2023), <https://www.hubengage.com/trends/harnessing-the-power-of-ai-in-human-resources/>

^{ix} Abdullah Malik, *Artificial Intelligence in Health and Safety*, SAFETYPEDIA (Feb. 22, 2023), <https://safetypedia.com/safety/artificial-intelligence-in-health-and-safety/>

^x Tristan Ovington, *7 AI legal issues and how to deal with them*, WALK ME BLOG (Nov. 22, 2023), <https://www.walkme.com/blog/ai-legal-issues/#:~:text=Examples%20of%20AI%20legal%20issues,Large%20fines>

^{xi} LexisNexis, *Top 8 Legal Areas Impacted by Generative AI: Where In-House Legal Teams Need to Focus*, WWW.LEXISNEXIS.COM (Aug. 31, 2023), <https://www.lexisnexis.com/community/insights/legal/b/thought-leadership/posts/top-8-legal-areas-impacted-by-generative-ai-where-in-house-legal-teams-need-to-focus>

^{xii} Clear Object, *How to Choose the Right AI Tools for Your Business*, WWW.CLEAROBJECT.COM (Jun. 6, 2023), <https://www.clearobject.com/how-to-choose-the-right-ai-tools-for-your-business/>

^{xiii} Hannah Malmstrom, *10 AI best practices for businesses: Using AI safely and ethically*, EDAPP (Sep. 18, 2023), <https://www.edapp.com/blog/ai-best-practices/>