Strategic AI Integration: Protecting Your Business from Emerging Legal Risks

Charles J. Vaccaro

Greenbaum, Rowe, Smith & Davis LLP Client Alert

May 28, 2026

What You Need to Know

- For businesses, the adoption of AI is not just a technological decision – companies using AI tools must be aware of potential legal exposure in areas including data privacy, intellectual property, employment practices, contractual liability, regulatory compliance, and confidentiality protections.
- To adopt AI in a responsible manner, businesses should proactively implement internal governance policies, employee training, vendor diligence procedures, and other protocols before routinely integrating AI into their operations.
- A strategic audit of current AI-related workplace practices can identify where AI usage may already be creating silent liabilities, better positioning a business to leverage the technology while minimizing avoidable exposure.

The adoption of artificial intelligence (AI) is rapidly transforming how businesses operate in nearly every industry sector. Companies are increasingly using AI to automate repetitive tasks, streamline customer service, analyze large datasets, improve marketing efforts, assist with drafting and document review, enhance forecasting, and support operational planning. As this technology continues to evolve, businesses that thoughtfully integrate AI into their operations may gain significant competitive advantages in both efficiency and scalability, resulting in substantial potential opportunities for companies that adopt it strategically and responsibly.

Adopting AI, however, is not just a technological decision, but also a legal one.

Attorneys

Charles J. Vaccaro

Key Legal Risks & Considerations

While AI can improve efficiency and reduce costs, it also introduces new risks related to data privacy, intellectual property, employment and HR practices, contractual liability, and regulatory compliance requirements. Understanding these risks and proactively addressing them is critical to avoiding disputes, unintended liability, and other adverse consequences.

The following, while not exhaustive, are among the most important legal issues that businesses must consider when incorporating AI into their operations:

Data Privacy & Confidential Information

The handling of sensitive data presents one of the most significant areas of legal exposure. Many business operating platforms rely on user inputs that may include customer data, employee information, financial records, proprietary strategies, and confidential contracts or communications.

If this information is uploaded to third-party AI systems without appropriate safeguards, companies may face risks such as:

- The breach of confidentiality obligations
- The violation of data protection laws
- A loss of control over proprietary information

Key takeaway: In New Jersey, businesses must be particularly cautious where contracts, employment agreements, or vendor relationships impose confidentiality obligations that may be implicated by AI use.

Intellectual Property Ownership

AI use raises complex questions involving ownership and control of work product. Key concerns in this area include:

- Whether AI-generated content qualifies for copyright protection
- Who has ownership of outputs generated using AI tools
- Whether AI training data infringes on third-party rights
- Whether business inputs become part of an AI provider's model or dataset

Key takeaway: Companies using AI to create marketing materials, software code, designs, or written content should carefully review the terms of service of AI platforms to understand how intellectual property rights are addressed. In certain instances, platform terms may grant providers broad rights over input and output data.

Employment Law & Workplace Use of AI

As employers increasingly incorporate AI into hiring, performance evaluation, and workforce management, several areas of legal exposure emerge:

- Bias and discrimination: systems trained on historical datasets may unintentionally produce discriminatory outcomes in hiring or promotions.
- Wage and hour compliance: automated scheduling or productivity tools may impact compliance with labor laws.
- Employee monitoring: AI-based surveillance or productivity tracking tools may raise privacy concerns.

Key takeaway: New Jersey-based employers must ensure that AI-driven employment decisions comply with state and federal anti-discrimination laws and do not inadvertently create disparate impact liability.

Contractual Liability & Vendor Concerns

Because most AI tools are licensed through third-party vendors, businesses must rely heavily on contractual provisions to allocate and manage potential risks. Key contract issues include:

- Indemnification provisions for IP infringement or data misuse
- Limitations of liability that may cap recovery in the event of significant harm
- Service level agreements (SLAs) regarding uptime and reliability
- Data security obligations and breach notification requirements

Key takeaway: Companies implementing AI tools without carefully reviewing vendor agreements may unknowingly assume significant liability exposure.

Accuracy, Hallucinations, & Reliance Risk

AI-generated outputs are not infallible and remain susceptible to incorrect or "hallucinated" outputs, which can lead to:

- Inaccurate legal or financial advice being relied upon internally
- Defective contracts or communications
- Misleading marketing statements
- Operational decisions based on incorrect data

In the legal context, AI tools have, in some instances, generated fictitious case citations, misstated legal standards, and fabricated quotations or authorities. Courts across the country have increasingly scrutinized attorneys and parties who submit AI-generated content without adequate verification.

Key takeaway: If a business relies on AI-generated output without appropriate human review, it may still be legally responsible for resulting harm. In regulated industries and litigation settings, failure to verify AI-generated information may also expose businesses and professionals to sanctions, malpractice claims, reputational harm, and other adverse consequences.

Regulatory & Compliance Considerations

Although AI regulation is still developing and remains fragmented, regulatory scrutiny is increasing at both the federal and state levels. Potential areas of concern include:

- Consumer protection laws prohibiting deceptive practices
- Data security and breach notification requirements
- Industry-specific regulations (healthcare, finance, insurance, legal)
- Emerging AI-specific regulatory frameworks

Key takeaway: Even in the absence of comprehensive AI legislation, existing laws still apply to AI-driven conduct and compliance requirements must be noted and observed.

Trade Secrets & Competitive Harm

AI tools can inadvertently expose sensitive business information if not properly controlled. Uploading proprietary data into external systems may risk:

- Loss of trade secret protection
- Unauthorized use of business strategies
- Exposure of confidential customer or pricing information

Key takeaway: Once confidentiality is compromised, legal remedies may be limited or difficult to enforce.

Attorney-Client Privilege & Discoverability in Litigation

The use of external AI platforms may also impact attorney-client privilege and the discoverability of sensitive information in litigation. Employees and executives increasingly use AI tools to summarize legal issues, review contracts, analyze disputes, or assist with internal decision-making. However, inputting privileged communications, work product, or sensitive legal strategy into third-party AI systems may jeopardize privilege protections depending on the circumstances, including how the information is stored, processed, or shared.

Additionally, prompts, inputs, and AI-generated outputs may later become relevant in litigation or regulatory investigations. Opposing parties and regulators may increasingly seek discovery concerning the use of AI tools used in connection with business decisions, compliance efforts, contract drafting, or internal communications. Businesses should therefore implement clear policies governing the use of AI in connection with legal matters and avoid uploading privileged or highly sensitive information into external

AI platforms without first understanding the legal and confidentiality risks associated with doing so.

Importantly, the law in this area is rapidly developing. For example, in *United States v. Heppner*, a federal court held that materials generated by a criminal defendant through a publicly available AI platform were not protected by attorney-client privilege or the work product doctrine. The court reasoned, in part, that communications with the AI system were not confidential and involved disclosure to a third party. While the decision was heavily dependent on specific case facts, it nonetheless highlights a growing concern that information entered into AI platforms may later become discoverable in litigation or lose confidentiality protections.

Key takeaway: Courts and regulators are only beginning to address how traditional doctrines involving attorney-client privilege, work product protection, confidentiality, and electronic discovery apply in the context of AI systems.

Risk Mitigation Strategies for Businesses

Companies adopting AI should establish governance procedures before integrating these tools into routine operations. Business owners and other decision makers should not assume that existing policies, contracts, or compliance procedures adequately address the unique risks associated with AI systems.

Clearly, internal AI governance policies are one of the most important effective risk-management tools. These policies should define:

- Which AI platforms employees are permitted to use
- What types of information may or may not be uploaded
- Approval procedures for AI-assisted work product
- Limitations on the use of AI in sensitive business functions

Employee training is equally important, particularly regarding confidentiality, data privacy, intellectual property, and accuracy concerns. Many AI-related risks arise not from the technology itself, but from employees using these tools without fully understanding their limitations, how they work, and the legal implications.

Careful vendor diligence is equally important. Before adopting an AI platform, businesses should review:

- Terms of service and ownership provisions
- Data retention and storage practices
- Confidentiality protections
- Security protocols
- Indemnification and limitation of liability clauses

- Whether user inputs may be used to further train the AI model

Companies should not assume all AI providers offer the same level of protection, as contractual safeguards and data handling practices can vary significantly between platforms.

Human oversight remains critical. AI-generated outputs should not be blindly relied upon for legal, financial, operational, or compliance-related decisions. Businesses should establish review procedures requiring qualified personnel to verify the accuracy and appropriateness of AI-generated content before it is implemented or distributed.

In addition, businesses should carefully evaluate how AI tools intersect with existing confidentiality obligations, contractual commitments, and regulatory requirements. Uploading customer information, proprietary business data, trade secrets, or privileged communications into external AI systems may create unintended legal exposure if appropriate safeguards are not in place.

Key takeaway: Companies should take proactive steps to identify and address the unique and specific legal, operational and regulatory risks associated with AI use.

Next Steps: A Strategy for Risk Mitigation

The most immediate AI-related legal exposure for many companies will not arise from the technology itself, but from informal employee use occurring faster than internal governance structures can adapt. Companies that implement clear policies, vendor diligence procedures, and review protocols early on will generally be better positioned to realize the operational benefits of AI while limiting avoidable litigation and regulatory exposure.

Businesses should closely review and protectively update all relevant procedures and protocols, including:

- Employment-related materials including policies and handbooks
- Confidentiality and other employment agreements
- Cybersecurity and technology usage policies
- External vendor contracts
- Data governance procedures
- Document retention and litigation hold practices

To facilitate this process, **an audit of current AI-related workplace practices** can identify where AI usage may already be creating silent liabilities, better positioning a business to leverage the technology while minimizing avoidable exposure.

It is worth noting that in some instances, the biggest risk may not come from the AI product a company purchases, but instead from the unapproved and/or unauthorized use of "free" unvetted AI tools by employees. This includes the use of public generative AI platforms accessed through personal accounts or

AI-powered browser extensions on work computers.

Legal guidance, including **a strategic review by knowledgeable counsel, is increasingly critical** as the legal and regulatory landscape surrounding AI continues to evolve. Businesses that proactively evaluate AI-related risks and implement thoughtful governance policies will often be in a significantly stronger position to leverage AI effectively while minimizing litigation, regulatory, and operational exposure.

Please contact the author of the Client Alert with questions or to discuss your specific business circumstances.

Charles J. Vaccaro
Partner, Litigation
cvaccaro@greenbaumlaw.com
732.476.3338