

Privacy and Legal Risks of Generative AI for Businesses

A Tishkoff PLC eBook



Tish.Law

Table of Contents

Introduction	01
Transparency in GenAI	02
Data Privacy and Security Risks	03
Intellectual Property Concerns	05
Legal and Ethical Considerations for Legal Professionals	06
Impact of Generative AI on Different Areas of Law	07
Regulatory Landscape and Best Practices	08
Conclusion	11
Contact Us	12
Further Reading	13

Introduction

Generative artificial intelligence (GenAI) is rapidly transforming the business landscape, offering unprecedented capabilities in generating text, images, and other content. While this technology presents exciting opportunities, it also introduces significant privacy and legal risks that demand careful consideration from business leaders.

This guide examines the key privacy and legal challenges associated with GenAI that business executives should be aware of when implementing AI solutions or facing AI-related disputes. Understanding these risks is crucial for protecting your business interests and knowing when to engage experienced business lawyers.

Forward-thinking business executives recognize that engaging business lawyers early in the AI implementation process can prevent costly disputes later. Expert business law attorneys can help establish:

- Comprehensive data governance frameworks
- Clear contractual terms with AI vendors and partners
- Robust compliance protocols for evolving regulations
- Strategic approaches to intellectual property protection

Don't wait for AI-related legal problems to impact your business operations. Connect with lawyers specializing in business law and AI today to safeguard your company's future.

Please note this eBook should be used for learning and illustrative purposes. It is not a substitute for consultation with an attorney with expertise in this area. If you have questions about a specific legal issue, we always recommend that you consult an attorney to discuss the particulars of your case.



Transparency in GenAI

Imagine a scenario where a lawyer relies on a GenAI tool to draft a legal document, only to discover that the tool has inserted fabricated case citations or misrepresented legal principles. This hypothetical situation highlights a fundamental concern with GenAI: the lack of transparency in how these models are trained and how they arrive at their outputs. Many GenAI tools are proprietary "black boxes," making it difficult to understand the underlying data and algorithms that drive their decision-making processes. This opacity raises concerns about potential biases, inaccuracies, and the risk of generating misleading or harmful content.



This lack of transparency poses challenges for legal professionals in ensuring compliance with ethical obligations and legal standards. For example, in a recent case, a lawyer was sanctioned for including fictional cases in his court pleadings, generated by a GenAI tool. This incident underscores the need for caution and critical evaluation when using GenAI in legal practice. The inability to fully understand how a GenAI tool arrives at its conclusions can have serious consequences for legal proceedings and a lawyer's professional reputation.

Data Privacy and Security Risks



Business Disputes

Construction and Real Estate Disputes

Employment Disputes

GenAI models are trained on massive datasets, often scraped from the internet, which may include personal and sensitive information. This raises concerns about data privacy violations, unauthorized access, and the potential for data breaches. These risks are particularly relevant in the context of business, construction, real estate, and employment disputes, where sensitive information is often involved.

- **Business Disputes:** In business disputes, the use of GenAI tools could lead to inadvertent disclosure of confidential business information, trade secrets, or sensitive employee data. For instance, if an employee uses a GenAI chatbot to summarize a confidential meeting and the chatbot inadvertently stores or shares this information, it could result in a data breach and legal liability. This risk highlights the need for businesses to implement robust data security measures and carefully consider the implications of using GenAI tools for handling sensitive information.
- **Construction and Real Estate Disputes:** Construction and real estate disputes often involve sensitive information related to property ownership, financial records, and contractual agreements. Using GenAI tools in these contexts requires careful consideration of data security measures and compliance with privacy regulations. For example, if a GenAI tool is used to analyze property records and inadvertently exposes sensitive financial information or personal data of property owners, it could lead to privacy violations and legal challenges.
- **Employment:** In employment disputes, the use of GenAI in hiring processes raises concerns about potential bias and discrimination. If a GenAI tool used for candidate screening is trained on biased data, it could perpetuate discriminatory practices and lead to legal challenges. For example, if a GenAI tool favors candidates from certain educational backgrounds or geographic locations, it could inadvertently discriminate against candidates from underrepresented groups, leading to potential legal action.





Intellectual Property Concerns

The use of copyrighted materials in training GenAI models raises questions about intellectual property infringement. If a GenAI tool generates content that closely resembles copyrighted work, it could lead to legal challenges and disputes over ownership.

For example, in the case of *Getty Images v. Stability AI*, Getty Images alleged that Stability AI used millions of copyrighted images without permission to train its Stable Diffusion image-generating tool. This case highlights the legal uncertainties surrounding the use of copyrighted materials in training GenAI models and the potential for litigation when intellectual property rights are allegedly infringed.

For a more detailed examination of the intersections of IP law and AI, read our Tishkoff e-Book “Intellectual Property Risks in the Age of AI,” on our website at tish.law/e-books/.

Legal and Ethical Considerations for Legal Professionals

The use of GenAI in legal practice raises ethical considerations for attorneys, particularly regarding confidentiality, competence, and supervision. Attorneys have a duty to protect client confidentiality, and using GenAI tools that store or share client information could violate this duty.

Furthermore, attorneys must ensure that they are using GenAI tools competently and that they are supervising the use of these tools by junior lawyers and staff. Relying solely on GenAI outputs without proper verification and human oversight could lead to errors, inaccuracies, and potential ethical violations.

For instance, if a business attorney relies on a GenAI tool for legal research and fails to verify the accuracy of the information provided, it could lead to misrepresentation of facts or legal principles, potentially harming the client's case.



Impact of Generative AI on Different Areas of Law

The increasing use of GenAI has the potential to significantly impact various areas of law, including contract law, intellectual property law, and employment law.

➔ Contract Law

GenAI can be used to draft and review contracts, potentially increasing efficiency and reducing costs. However, it also raises concerns about the enforceability of contracts generated by AI and the potential for errors or misinterpretations. For example, if a GenAI tool generates a contract with ambiguous clauses or inconsistencies, it could lead to disputes and challenges in court.

➔ Contract Law

➔ Intellectual Property Law

➔ Employment Law

➔ Intellectual Property Law

As discussed earlier, the use of copyrighted materials in training GenAI models raises concerns about intellectual property infringement. Additionally, the ownership of AI-generated content and the ability to copyright such content are still evolving legal issues.

➔ Employment Law

The use of GenAI in hiring processes raises concerns about bias and discrimination, as mentioned earlier. It also has implications for employee privacy, data security, and the potential for AI-driven surveillance and monitoring in the workplace.





Regulatory Landscape and Best Practices

The regulatory landscape surrounding GenAI is rapidly evolving, with jurisdictions like the European Union implementing regulations like the AI Act to address concerns about transparency, accountability, and risk management. This Act categorizes AI systems based on risk levels and imposes stricter requirements for high-risk AI systems, such as those used in critical infrastructure or law enforcement.

In the United States, agencies like the Federal Trade Commission (FTC) are actively investigating and enforcing existing laws related to data privacy, copyright, and consumer protection in the context of GenAI. The FTC has expressed concerns about the potential for GenAI to be used for deceptive or unfair practices, such as generating fake reviews or impersonating individuals.

To mitigate the privacy and legal risks associated with GenAI, businesses and legal professionals should adopt best practices.



Best Practice	Description
Data Minimization	Limit the collection and use of personal data to what is necessary for the specific purpose. For example, when using GenAI for candidate screening, collect only job-relevant information and avoid collecting sensitive data like age or race.
Transparency	Provide clear and accessible information about how GenAI models are trained and how they use data. This could include disclosing the types of data used for training and explaining the decision-making processes of the AI system.
Confidentiality	Implement robust security measures to protect confidential information and ensure compliance with privacy regulations. This may involve encrypting data, restricting access to sensitive information, and conducting regular security audits.
Accuracy and Verification	Verify the accuracy of GenAI outputs and avoid relying solely on AI-generated content. For example, when using GenAI for legal research, always cross-check the information with reliable sources and legal databases.

Best Practice	Description
Human Oversight	Maintain human oversight in the use of GenAI tools, especially in critical decision-making processes. This could involve having a human review AI-generated content or requiring human approval for certain AI-driven actions.
Bias Mitigation	Implement strategies to identify and mitigate potential biases in GenAI models. This may involve using diverse training data, regularly auditing AI systems for bias, and implementing fairness-aware algorithms.
Ethical Guidelines	Develop and implement ethical guidelines for the use of GenAI within the organization. These guidelines should address issues like data privacy, fairness, accountability, and transparency.
Stay Informed	Keep abreast of evolving regulations and best practices related to GenAI. This could involve monitoring regulatory developments, attending industry conferences, and consulting with legal experts.



Conclusion

GenAI presents both opportunities and challenges for businesses and legal professionals. By understanding the privacy and legal risks associated with this technology and adopting appropriate safeguards, organizations can harness the power of GenAI while mitigating potential liabilities. This requires a proactive approach to data privacy, intellectual property protection, and ethical considerations, along with a commitment to staying informed about the evolving regulatory landscape.

This white paper has highlighted key privacy and legal risks associated with GenAI, drawing upon research and insights from various sources. It has emphasized the importance of transparency, data security, and ethical considerations in the use of GenAI, particularly in the context of business, construction, real estate, and employment disputes. By implementing best practices and staying informed about the evolving legal landscape, businesses and legal professionals can navigate the challenges and opportunities presented by this transformative technology.



Questions about business law or litigation?

Contact Tishkoff

Tishkoff PLC specializes in business law and litigation. For inquiries, contact us at www.tish.law/contact/. & check out Tishkoff PLC's Website (www.Tish.Law/), eBooks (www.Tish.Law/e-books), Blogs (www.Tish.Law/blog) and References (www.Tish.Law/resources).

Tishkoff PLC
407 North Main Street
Ann Arbor, Michigan 48104

 Tish.Law

 tishkoffplc@tish.law

 855.TISH.LAW

Further Reading

Lee, H.-P., Yang, Y.-J., von Davier, T. S., Forlizzi, J., & Das, S. (2024). *Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks*. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)* (pp. 1–30). ACM.

Atkinson, D., & Morrison, J. (2024). *A Legal Risk Taxonomy for Generative Artificial Intelligence*. Allen Institute for Artificial Intelligence. 23 May 2024.

Iowa State Research. (n.d.). *Generative AI in Research: Guidance FAQ*. Iowa State University.

University of California, Davis Law Library. (February 12 2025). *Risks, Limitations, and Professional Responsibility – Generative AI Tools and Resources for Law Students*. UC Davis.

Toland, Stephen, et al. (July 9 2024). *Generative AI and Data Protection: What Are the Biggest Risks for Employers?* FBFK Law.

Waitman, Robert. (January 25 2024). *What Are the Privacy Risks of Generative Artificial Intelligence?* BizTech Magazine.

Deloitte AI Institute. (2023). *The Legal Implications of Generative AI*. Deloitte Legal.

Miller, Katharine. (March 18 2024). *Privacy in an AI Era: How Do We Protect Our Personal Information?* Stanford University Human-Centered Artificial Intelligence.

Thompson Reuters. (March 1 2024). *The Key Legal Issues Relating to the Use, Acquisition, and Development of AI*. Thompson Reuters Legal.

OpenText. (2024). *Generative AI Governance Essentials*. OpenText Media.

Neschke, Sabine. (January 18 2024). *Legal Challenges Against Generative AI: Key Takeaways*. Bipartisan Policy Center.

Volkov Law Group. (January 31 2025). *Embracing Generative AI: The Current Risk Profile*. JDSupra.

Ferris, Chris. (n.d.) *How Business Can Maximize Opportunities and Mitigate Risks When Using Generative AI*. Pierpont.