WHEN AI BACKFIRES

How to Protect Clients from Invisible Legal Risks

Joshua Heiman, CIPP/US Klinedinst PC

In recent years, artificial intelligence has become embedded in core legal, business, and operational functions across industries. From document drafting to website analytics to claims processing, AI tools are increasingly being used by legal teams, vendors, and clients alike. However, with that efficiency comes an evolving class of risk—legal, reputational, and regulatory.

While some failures may appear to stem from the AI tools themselves, the true cost is often borne by the client. Whether through litigation, sanctions, regulatory penalties, or business interruption, attorneys must be prepared to recognize, evaluate, and mitigate the legal fallout of AI failures. This article highlights several high-profile incidents that reveal common risk patterns, followed by key steps counsel can take to better protect their clients and organizations from similar outcomes.

KNOW THE TECHNOLOGY BEFORE YOU RELY ON IT

In *Mata v. Avianca, Inc.*, No. 22-cv-01461 (S.D.N.Y. June 22, 2023), an attorney submitted a legal brief drafted in part using OpenAI's ChatGPT. The brief included citations to six fabricated cases. After the court issued an order to show cause, the attorney admitted the filings had not been verified. The court ultimately issued sanctions against the attorney and his firm.

This case underscores a growing reality: generative AI tools can convincingly produce false or misleading outputs. When attorneys use these tools in drafting or research without human verification, clients may be exposed to judicial sanctions, malpractice claims, and reputational harm.

PRACTICAL TIP: Treat all AI-generated content—especially in litigation—as a draft requiring full legal vetting. Attorneys should be transparent with clients about AI use and maintain a human review record for risk management and ethics compliance (see ABA Formal Opinion 498, "Virtual Practice," 2021).

AI IN CLAIMS PROCESSING AND DENIALS

In a 2023 hearing before the U.S. Senate Committee on Finance, lawmakers scrutinized the use of AI-driven tools by Medicare Advantage insurers to issue automated denials for post-acute care. As reported by The American Journal of Managed Care, insurers used algorithms to deny medically necessary rehabilitation and skilled nursing coverage, often overriding physician recommendations and bypassing human review.

CLIENT IMPACT: Patients were discharged early or denied access to care, providers were exposed to liability for wrongful discharge, and insurers faced increasing litigation risk and federal oversight.

PRACTICAL TIP: Health care counsel should review AI-driven decision systems for compliance with federal insurance regulations and patient rights laws, including the Medicare Act and applicable state health codes.

CROSS-BORDER AI SYSTEMS AND DATA TRANSFERS

In *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* ("Schrems II"), Case C-311/18 (CJEU July 16, 2020), the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield framework for international data transfers, citing inadequate protections against U.S. government surveillance.

CLIENT IMPACT: U.S.-based companies processing EU personal data with cloud-based or offshore AI systems risked immediate GDPR violations, regulatory enforcement, and operational disruption.

PRACTICAL TIP: Counsel should conduct transfer impact assessments (TIAs) when cross-border data flows involve automated or AI-enabled decision-making.

TRAINING DATA AND BIOMETRIC PRIVACY

Clearview AI, Inc. scraped more than 3 billion facial images from social media and other public websites without user consent and built a facial recognition tool sold to law enforcement. The company faced multiple lawsuits under the Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14/1 et seq.

CLIENT IMPACT: Companies using AI vendors with improperly sourced data risk exposure under biometric privacy laws—even when not directly collecting the data themselves.

PRACTICAL TIP: Vendors must certify the lawful sourcing of training data. Clients should obtain written assurances regarding compliance with applicable privacy and biometric statutes.

CONSENT AND COMMUNICATION MONITORING

In *Javier v. Assurance IQ, LLC,* 78 F.4th 1134 (9th Cir. 2023), the Ninth Circuit held that obtaining consent after the start of a website visit was insufficient to satisfy California's Invasion of Privacy Act (CIPA), Cal. Penal Code § 631.

CLIENT IMPACT: Dozens of companies using chat widgets, behavioral tracking tools, or session replays have since been targeted by CIPA-based class action suits.

PRACTICAL TIP: Businesses must ensure they obtain explicit and informed user consent before beginning data collection or communication monitoring.

CONCLUSION: AI RISK IS MANAGEABLE—IF YOU KNOW WHERE IT LIVES

The legal issues surrounding AI are expanding as fast as the tools themselves. While the underlying technologies differ—natural language generation, predictive modeling, facial recognition, or automated decision-making—the risk categories are consistent: hidden bias, unvetted data flows, lack of transparency, and weak consent mechanisms.

Clients rarely know where AI is embedded in their systems or what their vendors are doing under the hood. Legal counsel must take a proactive role in identifying AI use cases, reviewing policies, and implementing contract language that anticipates potential liability.

With the right planning—focused on data mapping, contractual protections, oversight, and disclosure—companies can harness AI's potential while staying clear of its legal landmines.

Because when AI fails, it's not just code that crashes. It's trust. And litigation follows close behind.

This article is for general informational purposes only and is not intended to be legal advice. For advice about your specific situation, please consult a qualified attorney.

Joshua Heiman, CIPP/US, is AI Counsel at Klinedinst PC and a nationally recognized advisor on privacy, technology law, and emerging risk. He serves on the Board of the California Lawyers Association (CLA), the Executive Committee of the CLA Privacy Law Section, and is a delegate for the California Delegation to the American Bar Association (ABA). Joshua counsels clients on legal exposure stemming from artificial intelligence, cross-border data transfers, and third-party vendor systems. He frequently speaks and writes on AI governance, litigation strategy, and regulatory compliance.