

# Artificial Intelligence Copyright Analysis and Fiduciary Considerations

Paul J. Morrow

Husson University, Bangor, USA

This paper explores the dimensions of Artificial Intelligence Law and Breach of Fiduciary duty when using AI research models. The paper also explores Artificial Intelligence in the international realm providing a basis for educating international firms. Reading this paper is worth your time because: (1) you will learn about copyrights and artificial intelligence; (2) you will also learn about artificial intelligence and the fascinating developments in money and banking; (3) you will read about the best practices in the disciplines, and international firm concerns and applications of U.S. AI dispositions. This paper will give you parameters so that one may navigate the legal landscape to help you plan and avoid the courts. As we all know, inflation is prevalent, and the best use of resources is essential to stay in business avoiding closure. Those firms domestic and global, who are not aware of the dangers suffer the perils that follow poor resource management practices. Our corporate psychologists and organizational managers heartily agree.

*Keywords:* copyright, AI and negligence, AI and regulation and fiduciary duty

## Introduction

The Copyright Laws and the regular garden variety breach of fiduciary duty for professionals managing other people's money is a serious topic regarding artificial intelligence. Within the past year or so, the law and management are focusing more on these two particularly important topics with significant developments. Increasingly, we see artificial intelligence involved in spanning the variety of literature to gather information for its database. Also, when professionals manage other people's money, artificial intelligence permeates our society. As corporate managers and international businesspeople, it does behoove us to know the risks and teach best practices. From my practicing law, this strategy of teaching and risk prevention was extraordinarily successful for all concerned. Remember that the human endeavor is to build trust and not to destroy. When cases are going to court, it's inefficient and cumbersome.

## Copyright Law and AI

The problem with generative AI is that it scans the information environment for information regarding certain subject matters. The very existence of generative AI is research based. For example, if you were to use AI to generate content-based marketing, the information would come from copyrighted material across the span of marketing information available in that vast spectrum. AI is then trained by that research material. Use of that research material, copied by AI, is a potential violation of copyright laws. Lawsuits are popping up everywhere

because the use of this research material is unauthorized by the owner of the copyright. The major legal question is: does the use of the copyrighted material qualify as fair use? Twenty-five to thirty lawsuits are currently pending in Federal District Courts in the U.S. Here are some of the leading cases and contextual analysis. Here are some recent AI copyright cases that have shaped the legal landscape:

### **Background: Thomson Reuters v. Ross Intelligence**

Thomson Reuters owns Westlaw, which is one of the largest legal research platforms in the world. Lawyers and other legal professionals pay Westlaw a subscription fee to access case law, state and federal laws, state and federal regulations, and law journals from Westlaw's website. Westlaw also contains its own editorialized content called "headnotes", which are short one-sentence summaries of key points of law or a court's decision. Ross Intelligence is a startup and competitor to Westlaw that used AI to train its legal search engine. Ross trained its AI by: (1) slightly rewriting Westlaw's headnotes into the form of a question; and (2) inputting these revised questions into its AI model.<sup>[3]</sup> Thomson Reuters discovered that Ross used its headnotes to train its AI model, and Thomson Reuters sued for copyright infringement. The Court concluded that Ross committed direct copyright infringement, finding it copied and materially appropriated Westlaw's headnotes. Ross argued that, despite any alleged copyright infringement that may have occurred, its actions were protected by fair use. (Healey, 2025)

When evaluating the fair-use defense, courts typically consider four factors: (1) the use's purpose and character, including whether it is commercial or nonprofit; (2) the copyrighted work's nature; (3) how much of the work was used and how substantial that part is, relative to the copyrighted work's whole; and (4) how Ross' use affected the copyrighted work's value or potential market. In *Thomson Reuters v. Ross Intelligence*, the Court explained that it was going to give the most weight to the first and fourth factors. (Healey, 2025)

### **Central Issue Disposition of Thomson Reuters v. Ross Intelligence**

The Federal District Court for the Eastern District of Pennsylvania (the Court) ruled that the defendant-AI developer's use of copyrighted material as training data for its AI model was: (1) a copyright violation and (2) not protected by fair use. The Court justified its fair use decision by reasoning: (1) the AI developer used copyrighted material to create a product that directly competed with the copyright holder; and (2) the AI developer's use of the copyrighted material would undermine the copyright holder's ability to license its data to other companies to train AI. The Court's decision raises concerns that fair use may not be a viable defense for AI developers in future lawsuits brought by copyright holders. AI companies should be aware of provisions within insurance policies that bar or limit coverage for copyright lawsuits. (Healey, 2025)

This case and several others offer especially useful insights as to the dispositive nature of the legal liability issues involving artificial intelligence and copyright law. We are in a new age of information gathering research and service. Many of these cases have not even been made to the Supreme Court. Another demonstrative illustration of artificial intelligence violating federal copyright statutes is *Concord Music Group, Inc. v. Anthropic PBC* (2025).

### **Central Issue Disposition of Concord Music Group, Inc. v. Anthropic**

District court grants motion to dismiss music publishers' claims of contributory and vicarious copyright infringement with leave to amend, and denies publishers' motion for preliminary injunction, finding that allegations that unidentified users might prompt AI product to produce copyrighted lyrics were insufficient to establish third-party infringement and that injunction sought was overbroad and not necessary to prevent irreparable harm. (Hussain & Gordils, 2025)

Plaintiffs are a group of music publishers, led by Concord Music Group Inc. and Universal Music Corp., that brought claims for direct and secondary copyright infringement and removal of copyright management information (CMI) against Anthropic PBC stemming from the use of Anthropic's signature AI product line, Claude. Plaintiffs alleged that Anthropic infringes their exclusive rights to musical lyrics by using their works to train Claude, and by distributing the lyrics in Claude's outputs when Claude is prompted. Plaintiffs sought a preliminary injunction to prohibit Anthropic from using the copyrighted lyrics for training purposes. Anthropic moved to dismiss plaintiffs' claims for contributory and vicarious infringement and the intentional removal of CMI and opposed plaintiffs' motion for a preliminary injunction. The court found in favor of

Anthropic in two consecutive decisions: first, denying the motion for a preliminary injunction as overbroad and failing to establish irreparable harm, and second, granting Anthropic's motion to dismiss with leave to file an amended complaint. In granting the motion to dismiss, the court found that plaintiffs failed to show any direct third-party infringement, i.e., that users submitting prompts actually generated copies of copyrighted lyrics, and that Anthropic knew or had reason to know of any third-party infringement. The court also found that plaintiffs did not sufficiently allege that Anthropic acted intentionally as to the removal of CMI, particularly given plaintiffs' acknowledgment that CMI was not removed across the board throughout Claude's training process. Prior to the court's decisions, the parties entered into a joint stipulation by which Anthropic agreed to maintain already implemented guardrails as to its current AI models and products. (Hussain & Gordils, 2025)

Plain and simple. If a firm is using AI, gathering information to sell the information or a service, be sure to get the consent and/or pay for the information. Otherwise, the firm is violating the copyright laws. To complicate matters further if artificial intelligence is generating a machine learned product, the information may not be copyrighted because the Copyright Act of 1976 requires human authorship. The following cases suggest that the debate is fervent and ongoing.

*Thaler v. Perlmutter* affirms the central place of the human being in copyright's doctrinal architecture. The D.C. Circuit proclaims that machines are mindless tools which do not need incentives nor possess subjectivity, downplays the importance of corporations in modern copyright law, and emphasizes the public benefit. The court makes equally clear that neither this decision nor the human authorship requirement will pose practical obstacles to the growing importance of AI-driven cultural production. In this way, the judgement continues the legacy of *Bleistein v. Donaldson Lithographing Co.* and *Feist v. Rural*, known for exalting authorial creativity while in fact lowering standards, focusing on economic growth, and in *Bleistein's* case, hiding the work for hire behind personality language. I expect the upcoming *Allen* case to take this up even further—both affirming the human authorship requirement as a matter of formality and depriving it of any substantive weight. (Błaszczuk, 2025)

So as to avoid all of this, firms can manage much better. The aforementioned cases arose and caused major inefficient use of resources because the matters went to court. The following suggestions on good practices and education is a better move toward profitability which is laid out properly in your firms.

### **Corporations Reinforce and Police AI Related Issues in an AI World**

To help employees create AI-assisted work materials that qualify for copyright protection, consider implementing these five guidelines: 1. **Ensure Active Human Participation in the Creative Process.** Employees should be actively involved in the creative process. The AI tools they use should assist and enhance their creative process, not replace it. Make sure your employees provide meaningful contributions to the final work product, and their personal input and decision-making should be evident. This means going beyond merely inputting prompts into an AI tool; they should actively shape, edit, and refine the output to reflect their unique contributions. Employees should also create works that are new and not derivative of existing works. Even when drawing inspiration from other sources, make sure their work adds new expression or meaning. Since the concept of "active human participation" in AI-assisted creations can be nuanced, you can provide employees with practical examples to help them understand the distinction between protectable and non-protectable AI-assisted works. 2. **Require Documentation.** Make sure your employees keep detailed records of their creative process, especially when using assistive technologies. This documentation can serve as evidence of authorship and the originality of the work. These records should include the specific AI tools used, the nature and extent of the AI's contribution, the prompts used with the AI tool (if feasible), and the employee's creative inputs and modifications to AI-generated content. 3. **Train Your People.** You should offer training sessions on the effective and lawful use of AI

tools in content creation. Let your employees know that works generated entirely by AI without significant human authorship may not be eligible for copyright protection. At this training and at all times thereafter, encourage your employees to consult the Legal/Compliance Department if they have questions about the use of AI in their work.

4. Create and Require a Review Process. All AI-assisted works should undergo a review process to confirm that they meet the company's standards for originality and creativity. You should designate a department or individual responsible for evaluating the human authorship present in the work and ensure compliance with company policy.

5. Develop a Company Policy on AI Use That Boosts Copyright Protections. To formalize these guidelines, HR managers and in-house counsel should collaborate to develop a comprehensive company policy on the use of AI tools in content creation. This policy should:

- Define Acceptable Use of AI Tools: Clearly outline how employees are permitted to use AI tools in their work.
- Establish Procedures for Documentation: Detail the requirements for documenting the creative process when AI tools are used.
- Set Standards for Human Authorship: Specify the level of human involvement required in AI-assisted works to qualify for copyright protection.
- Outline the Review and Approval Process. Describe the process for reviewing AI-assisted works to ensure compliance with company standards and copyright laws.
- Provide Resources for Training and Support: Offer information on available training sessions and designate contacts within the appropriate department for employees seeking guidance.

As AI continues to fuel the creation of work product, companies must implement clear guidelines and policies to ensure the materials are eligible for copyright protection. By actively engaging in the creative process, documenting their work, and adhering to company policies, employees can effectively use AI tools while safeguarding the company's intellectual property rights. (Kahn & Walters, 2025)

### **Violation of the Copyright Act, or Any Regulation of AI That Amounts to Damages Is Negligence.**

In addition to the violation of the Copyright Act, a separate cause of action in the pleadings arises in Negligence: and is Negligence per se. That is, the breach of the duty of reasonable care which is the proximate cause of damage to the person affected, the Plaintiff. All the Plaintiff has to do is to show that the statute or the regulation has been violated. That is enough proof for negligence per se. After proof of the violation of the statute, the court moves to damages. In the previous examples given, all the Plaintiffs have a count or cause of action in negligence in the pleadings. The way lawsuits are filed is that a multi-page document called the Plaintiff's complaint is served upon the Defendant and filed with the court albeit if it is a Copyright action concurrently with the Federal District Court. The negligence cause of action allows a Plaintiff to recover tons of damages usually much more than the damage caused by the violation of the copyright act. Lost profits, Lost compensation, and Punitive damages can be more extensive running into the millions because the degree of foreseeability extends farther into the future than the scope that most statutes allow. Also, any violation of any regulation amounts to negligence per se. When I was in private practice, it was customary and usual to plead a count in negligence for the violation of a statute, or regulation. Once proven, the rest is easy. All the Plaintiff needs to show is that they suffered the harm.

It behooves a corporation to have a strategy to manage AI. From auditing AI users, to providing content credentials, to training in AI, and regulatory education, multinational corporations must authenticate employee training to avoid vicarious liability for violating any statute or regulation.

### **Banking, Investments, and AI Start With the General Theory of Breach of Fiduciary Duty and Regulation**

In order for a bank to be sued over AI related activity a Plaintiff must show that there is a fiduciary or special relationship with the client. Usually this involves a bank deposit customer, a trust department client, or the bank

serving as investment broker or personal financial advisor to the client. The Plaintiff must show that the bank used AI and that the AI provided misleading, false, or unreasonable information. The Plaintiff must show that the AI harmed the client. The client can recover investment losses and emotional suffering. Wall Street banks use algorithms without doing their homework, or following proper investment protocol after using AI, leading to losses. Here are some real situations and cases involving AI in financial services. This first illustration communicates that Directors of the bank are vulnerable to AI negligence in banking.

The lawsuit names 11 directors and six officers as defendants, including former CEO Gregory Becker, former CFO Daniel Beck and former chief risk officer Laura Izurieta, whom the FDIC asserts repeatedly ignored red flags, including violations of the bank's internal risk models, as interest rates rose.

The FDIC noted mismanagement of the bank's held-to-maturity securities portfolio in 2021. The officers and directors pursued higher yields by heavily investing in long-term, unhedged securities despite obvious interest rate risks, ignoring recommended exposure limits, and repeatedly violating internal risk policies, the FDIC asserted. The officers manipulated risk model assumptions to mask policy breaches instead of addressing these issues, the agency said.

FDIC Chair Martin Gruenberg, in a December memo, said the agency's board was considering a request for authority to sue six former officers and 11 former directors of SVB to hold them accountable for their mismanagement of the bank's investment portfolio that "exposed SVB to significant risks, caused SVB to incur billions of dollars in losses, and resulted in a loss to the Deposit Insurance Fund currently estimated at \$23 billion."

The FDIC complaint comes nearly two years after SVB's failure, the third-largest bank failure in U.S. history. SVB's total assets more than tripled in three years—growing from less than \$60 billion at the end of 2019 to \$209 billion at the end of 2022. At that time, SVB noted in its call reports that 94% of its deposits were uninsured and the influx of deposits was largely invested in long-duration securities, the FDIC noted. (Chakravarty, 2025)

These are serious matters that involve Attorney Fees, Time, and damages to be collected from the directors of the corporation. Risk management teams must be initiative-taking.

Also, AI can initiate fraudulent transfer of funds. For the deposit customer, voice activated systems are in use to transfer funds from one account to another. For example, all one has to do is to initiate contact with the bank, give the automated teller the instructions using voice-activated systems, and funds can be transferred. This AI process is being challenged by a man in Texas who was robbed of funds by someone who mimicked his voice, and fraudulently transferred money, stole money from the customer. The bank is being sued for not providing proper safeguards against the AI voice command. This is a violation of banking regulations and therefore is a case for negligence per se against the bank. The bank manager and the directors are also potentially responsible.

The most notable recent case in Texas, Gary Cunningham vs. PlainsCapital & Pathward N.A. involves AI voice recognition and the fraudulent transfer of funds, Gary Cunningham, a 76-year-old Houston resident who is suing two banks after fraudsters convinced an accountant to impersonate his voice, transferring \$20,000 from his account to another account. Because the bank did not have the adequate safeguards to protect the AI intruders, the court ruled in favor of Cunningham. This case raises many problems with breach of AI systems involving not only voice activated AI systems, but the use of AI in general in banking. Imagine the chaos of losing the money in your checking account and the hassle of having to file a lawsuit to get your money back. Texas has biometric law. The name of the statute is Capture or Use of Biometric Identifier Act (CUBI). Within the provisions of this statute, notice and consent are required before the collection and use of biometric data. The judge in this case ruled that the claim of gross negligence be submitted to arbitration and dismissed the pending legal action. Cunningham was trying to recover his \$20,000 and to protect senior citizens from scams. AI arbitration was the subject of one of my prior research papers and remains a viable alternative to litigation.

The breach of fiduciary duty is gaining popularity among investors where the stakes are high. In a case of first impression, *Spence v. American Airlines, Inc.*, pension participants sued Blackrock, an investment advisory firm, for breach of fiduciary duty because of too heavy a concentration in ESG investments. Blackrock used AI algorithm systems to help conduct its investment research. The ultimate disposition of the case was that the investment firm breached its duty of loyalty within the provisions of ERISA. The pension plan did not include ESG type investments. The federal judge ruled that it is a breach of fiduciary duty when investment banks lose money on behalf of clients when the funds invested are not aligned with the plan documents. One would recall that ESG investing was in fashion during the Biden administration and plummet after President Trump got elected. Investment firms must strictly act solely for the benefit of the beneficiary avoiding unbalanced investments.

Investment firms use AI-powered investment data gathering systems that must be supervised and executed in line with the investment objectives of the client. When people make money, the practice is not questioned. When people lose a lot of money, the issue makes it to the forefront. Also worth mentioning is that the directors of the corporation charged with supervising the AI policies of the corporation would be implicated.

Our society is changing rapidly. Here are some other non-exhaustive topics related to AI. As mentioned, AI is used to maximize investment strategies. AI is also used in credit scoring. Recent allegations that have prop up involve accusations of discrimination in credit worthiness. AI is also replacing people in banking. Hundreds of people in banking are being laid off because of AI systems. Banks in particular must be careful because AI does suggest certain investments that involve bias in decision making breaching fiduciary duty. Deregulation is the current theme in banking. That may not be a good turn of events. Unsupervised AI, or Blackbox reliance on AI presents sublime risk to financial institutions who use AI to improve decision-making and create better efficiencies. The complexities are far reaching. Litigious plaintiffs want their money back in situations involving AI and insurance companies offer AI related coverage. Flawed log rhythms aside, as well as other problems create undetected risk hiding and waiting to emerge. In response to all of this, management must institute systems of risk management.

Using AI has the potential to transform data management practices, but it also comes with its own set of challenges. Some of the major challenges faced in using AI for data management include:

- Data quality: AI algorithms heavily rely on the quality of data used for training and analysis. If the data is inaccurate, incomplete, or biased, it can lead to erroneous results and decisions.
- Data privacy and security: With the increasing use of AI in data management, ensuring the privacy and security of sensitive information has become a major concern. Organizations must implement robust security measures to protect their data from cyber threats.
- Lack of skilled workforce: Building and maintaining AI systems requires specialized skills and expertise. However, there is a shortage of skilled professionals with knowledge in both AI and data management, making it challenging for organizations to leverage AI effectively.
- Ethical concerns: With the increasing use of AI in various industries, ethical considerations have become a crucial aspect. Organizations must ensure that their AI systems adhere to ethical guidelines and do not discriminate against any group or individual.
- Integration with existing systems: Implementing AI systems also requires integration with existing systems in an organization. This can involve additional costs and challenges, but it is necessary for the seamless functioning of AI technology within an organization.

To tackle these challenges, businesses can deploy purposeful strategies. (Chia, 2025)

## **Data Centralization**

Break down silos by creating a centralized data repository. This unified access ensures that data is managed efficiently and used effectively across the organization. This repository makes it easier for AI to be applied

directly on, without having to combine datasets across platforms.

Centralized data repositories can come in the form of:

Data lakes: A large, centralized repository that stores both structured and unstructured data for analysis.

Data warehouses: A database designed to store and manage large volumes of data from various sources.

Data lake houses: A hybrid approach that combines the features of data lakes and warehouses.

These centralized repositories can also provide security measures to protect sensitive data, as well as tools for data governance and compliance. With a centralized repository, organizations can have greater control over their data and ensure consistency across different departments and systems.

For example, you can use data lakes or data warehouses equipped with AI functionalities like Snowflake or Google BigQuery to store and manage large datasets seamlessly. (Chia, 2025)

### **Annotation and Labeling**

High-quality labeled data is the foundation of good AI training. When working with AI systems for use in data management, data labeling is an essential step in the process. It involves identifying and tagging specific data elements with relevant categories or attributes to make them easily recognizable by AI algorithms.

There are several types of data labeling, each suited for different purposes and datasets:

Supervised labeling: This type of labeling is used when there is a pre-defined set of labels or categories that the data needs to be classified into. Human annotators manually assign these labels to the data, providing a ground truth for the AI system to learn from.

Semi-supervised labeling: In semi-supervised labeling, only a subset of the dataset is labeled, while the rest is left unlabeled. This approach is useful when there is a large amount of data to be labeled, and manually labeling all of it would be time-consuming and expensive.

Unsupervised labeling: Also known as self-labeling or automatic labeling, this type of labeling involves using algorithms to automatically assign labels to the data based on patterns and similarities in the dataset. It does not require human annotation, making it a cost-effective option for large datasets.

Active learning labeling: Active learning combines elements of supervised and unsupervised labeling by allowing human annotators to interact with the AI system during training. These annotations and label will help boost AI performance, leading to better data quality. (Chia, 2025)

### **International Collaboration Is Necessary**

Nothing is more important than the international perspective. This is the venue where universal truths are debated, and problems are resolved for the good. Regarding AI, international firms do not face the regulatory landscape that they face in Europe and elsewhere. That said, it is important to take in the international sector.

### **Establishing the Regulatory Framework**

In the absence of a global AI compact, we are seeing the emergence of divergent regulatory approaches—for example, the United States’ market-based model, the European rules Union’s based approach, China’s state-led approach, and India’s “hybrid” model, among others. While some variation is expected on issues such as privacy and copyright, too many deviations at the national level are likely to create regulatory fragmentation and affect global businesses.

Therefore, arriving at a shared understanding of the risks involved—both near-term and long-term risks to humanity—is necessary. A global AI compact would help identify these risks, frame regulatory principles, and recommend effective oversight and enforcement mechanisms.

What Will It Achieve? Going back to the question at hand, below are five outcomes a global AI compact would achieve.

**Common standards:** A global AI compact would reduce fragmentation by promoting interoperability through common standards. For example, a standard definition for “foundation models” and appropriate safety benchmarks to regulate the deployment of these models would benefit national regulators as they translate global principles into domestic policy. A global compact would also establish a neutral international body to develop such standards and update them based on regular evaluations.

**Ethical principles:** Responsible AI norms ensure that AI systems are designed, deployed, and implemented at an organizational level with certain ethical considerations in mind. A global AI compact would ensure that fairness, accountability, transparency, and other key principles are reflected in responsible AI frameworks around the world, irrespective of the political and social values of a particular government or institution.

**Research and innovation:** A global AI compact would incentivize open access to research and foster a collaborative ecosystem. This will, in turn, enable industry, academia, and startups from around the world to invest in innovation. Although some countries are likely to pursue sovereign AI goals, a global AI compact would facilitate cross-border collaboration, knowledge sharing, and mentorship.

**Equitable access:** A global AI compact would encourage nations to share resources and develop solutions to decentralize AI infrastructure. International cooperation would also resolve supply chain constraints, promote the movement of workforces across borders, and democratize access to critical resources.

**Workforce development:** A global AI compact would also support international efforts to train the workforce in the skills required to participate in an AI-driven economy. (Mohanty, 2024)

### **The Role of Global Institutions**

Developing a global AI compact is a multistage process that requires the involvement of multiple stakeholders. Identifying the role of each of these stakeholders is an important first step.

For example, the G20, with the African Union as a permanent member and Brazil as its sitting president, plays a vital role in representing the interests of the Global South. On the other hand, the GPAI can help in the harmonization of data governance and responsible AI frameworks.

To make the process more inclusive, representatives from technical bodies such as the Internet Engineering Task Force, the Institute of Electrical and Electronics Engineers, and the International Organization for Standardization should be involved. Additionally, the World Intellectual Property Organization can offer advice on standards and regulations.

Over time, specialized forums may be required to discuss specific issues such as military applications of AI, trust and safety, or trade, labor, and antitrust issues. With a clear mandate for each institution, a global AI compact will be closer to reality and much more likely to succeed. (Mohanty, 2024)

### **Conclusions and Recommendations**

1. Permission and consents must be obtained to avoid infringement of copyrighted materials for AI purposes.
2. The Directors of a Corporation must be kept informed regarding corporate AI uses by the company.
3. The Federal Trade Commission needs to be prompt in AI negligence related cases.
4. For international partners to come to America, we need global AI research and instruction.
5. Continue to educate and work together to develop AI within a good legal, responsible framework.



## References

- Blaszczyk, M. (2025). Thaler v. Perlmutter: Human authors at the center of copyright? Kluwer Copyright Blog. Retrieved July 15, 2025 from <https://copyrightblog.kluweriplaw.com/2025/04/08/thaler-v-perlmutter-human-authors-at-the-center-of-copyright>
- Chakravarty, R. (2025). FDIC sues 17 ex-SVB executives in alleged “gross negligence”, Banking Dive. Retrieved July 16, 2025 from <https://www.bankingdive.com/news/fdic-sues-17-ex-svb-executives-in-alleged-gross-negligence/737712/>
- Chia, A. (2025). AI data management: Strategies, tools, and trends. Retrieved August 9, 2025 from [https://www.splunk.com/en\\_us/blog/learn/ai-data-management.html](https://www.splunk.com/en_us/blog/learn/ai-data-management.html)
- Healey, C. (2025). Briefings, Takeaways from Thomson Reuters v. Ross Intelligence: AI litigation risks and insurance solutions. Retrieved July 15, 2025 from <https://briefings.brownrudnick.com/post/102k566/takeaways-from-thomson-reuters-v-ross-intelligence-ai-litigation-risks-and-insurance>
- Hussain, S., & Gordils, C. (2025). Concord Music Group, Inc. v. Anthropic PBC. Retrieved July 15, 2025 from <https://www.loeb.com/en/insights/publications/2025/04/concord-music-group-inc-v-anthropic-pbc>
- Kahn, A., & Walters, D. (2025). 5 steps you can take to ensure your company’s ai-generated works are protected by copyright, insights. Retrieved July 16, 2025 from <https://www.fisherphillips.com/en/news-insights/companys-ai-generated-works-are-protected-by-copyright.html>
- Mahanty, A. (2024). Why we need a global AI compact. Retrieved August 9, 2025 from <https://carnegieendowment.org/posts/2024/03/why-we-need-a-global-ai-compact?lang=en>