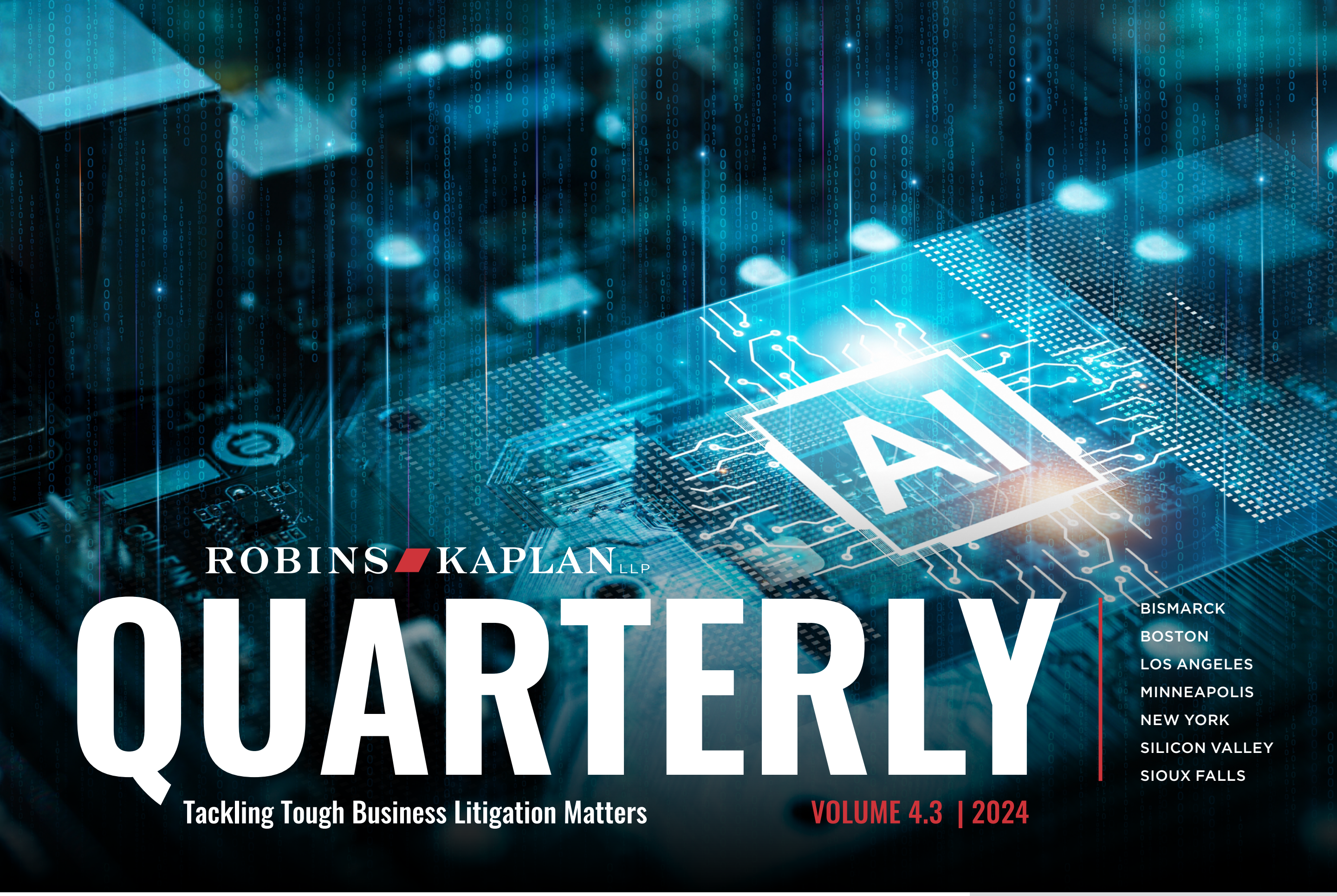


ROBINS KAPLAN LLP

QUARTERLY

Tackling Tough Business Litigation Matters

VOLUME 4.3 | 2024

BISMARCK
BOSTON
LOS ANGELES
MINNEAPOLIS
NEW YORK
SILICON VALLEY
SIOUX FALLS

Litigation Perspective: Strategies for Licensing Software that Leverages Artificial Intelligence

BY BRYAN MECHELL AND NAVIN RAMALINGAM

INTRODUCTION

As software products and services increasingly take advantage of the emerging capabilities of artificial intelligence (AI), software developers and companies that license software face evolving legal risks and contractual considerations. Software developers and licensees that fail to negotiate clear software license agreements that account for unique aspects of licensing AI-powered software may find themselves facing unexpected liability or costly software license dispute litigation. When drafting and negotiating software license agreements, parties should carefully consider the legal implications of developing and using software that incorporates AI.

READ MORE ON PAGE 2

IN THIS ISSUE:

Litigation Perspective

Bryan Mechell and Navin Ramalingam dive into strategies for licensing software that leverages artifical intelligence.

COVER ARTICLE

AI's Impact on Property Insurance Coverage

Learn more about how AI is revolutionizing property insurance.

PAGE 10

Front and Center

The latest and greatest at Robins Kaplan.

PAGE 18

Featured Appellate Results

PAGE 20

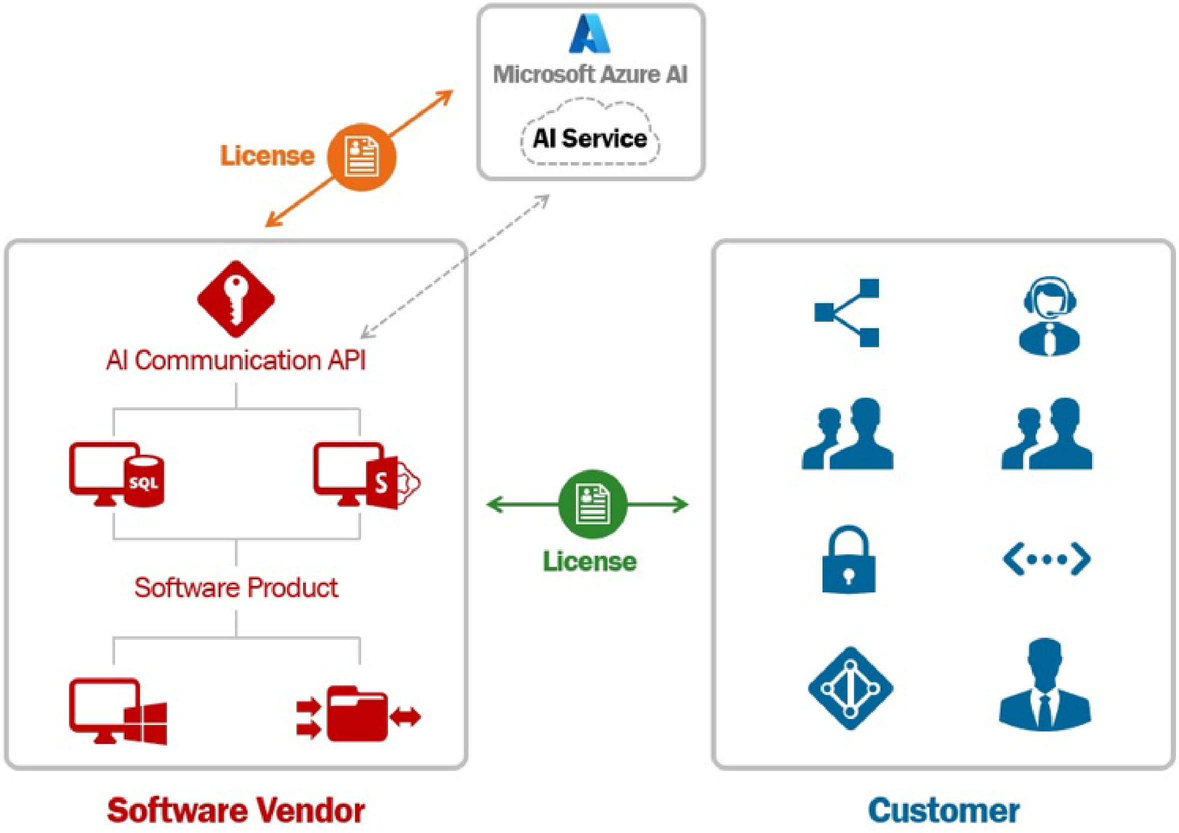
Software developers and licensees encounter two common types of AI-powered software products implicated in licensing agreements: (1) software products that leverage third-party AI services hosted offsite; and (2) software products that leverage custom-built AI, deployed either in the cloud or within on premises infrastructure. Each type of AI integration gives rise to important strategic considerations and risks that stem from using AI services, including intellectual property rights, data privacy, security and breach concerns, gatekeeper responsibilities, service performance guarantees, and evolving legal and regulatory landscapes. In this article, we discuss important issues parties should consider when negotiating master service agreements (MSAs), statements of work, and other license agreements that involve AI. This article also offers insights and recommendations to proactively manage risks and negotiate favorable contract terms.

SOFTWARE PRODUCTS THAT LEVERAGE THIRD-PARTY AI SERVICES

Software companies rely upon powerful AI services from tech giants like Microsoft, Google, and Amazon to enhance their products with capabilities such as natural language processing (NLP) and predictive analytics. While incorporating third-party AI services can provide compelling features, professionals tasked with managing licensing of these assets should carefully consider potential risks associated with their use.

The following figure illustrates a scenario where a customer licenses software from a Software Vendor that leverages third-party AI functionality—in this example, an OpenAI large language model (LLM) running on Microsoft Azure.

When drafting and negotiating software license agreements, parties should carefully consider the legal implications of developing and using software that incorporates AI.



In the above example, the Customer has a software license agreement that addresses the scope of the relationship with Software Vendor, as well as a separate agreement with Microsoft that addresses the scope of services provided by Microsoft Azure. On top of that, OpenAI publishes a list of representations and promises describing how it uses (or does not use) client data in connection with the OpenAI LLM. The Software Vendor, Microsoft, and OpenAI all provide some form of functionality relating to the software product licensed by the Customer, which includes handling and processing confidential customer data. This raises important considerations when licensing the software product, including allocation of liability relating to software functionality, responsibility for data privacy and security, and IP rights.

ERRORS OR DAMAGES CAUSED BY THIRD-PARTY AI

Consider the following hypothetical. A healthcare software company that sells its products to hospitals and medical service providers uses a third-party AI model, like Google Vertex AI, to analyze medical images for early disease detection. Due to issues with how the AI model was trained, the software misclassifies thousands of X-rays—leading to numerous false positives, unnecessary patient anxiety, follow-up tests, and in a few cases, unneeded invasive procedures. Even if the healthcare software company includes a "reliance" clause in its license agreement—stating, for example, that the software provider cannot guarantee the accuracy of third-party AI services—a court may still impose a duty on the healthcare software company as an "informed intermediary" with specialized knowledge in AI and healthcare to protect end-users from known risks in AI technology. *See Moll v. Intuitive Surgical, Inc.*, 2014 WL 1389652, at *4 (E.D. La. April 1, 2014) (holding that using a software product like a medical robot does not remove the software user / service provider from the scope of liability). By deciding to integrate a particular AI service, the healthcare software company could be seen as endorsing its capabilities. It is therefore critical that software developers not only include license terms addressing third-party AI functionality, but also carefully consider potential legal risks where special duties may attach.

DATA PRIVACY AND SECURITY RISKS

When a software product or service integrates with a third-party AI service, data flows in multiple directions—(1) from software vendor systems to AI, through their AI models, and back again; and (2) from software vendor systems to client systems, and back. This expanded data journey can increase privacy and security risks.

Looking at Microsoft Azure as an exemplar, Microsoft states that Azure OpenAI maintains strict data privacy and security measures for customer interactions. *See* DATA, PRIVACY, AND SECURITY FOR AZURE OPENAI SERVICE, https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy. Microsoft also represents that customer prompts, completions, embeddings, and training data are kept confidential and are not shared with other customers, OpenAI, or used to improve any models or services. While Azure OpenAI handles prompts, generated content and data, Microsoft states that it does not use this information to automatically enhance models. Customers can fine-tune models with their own data, but these customized models remain exclusively available to the specific customer who created them.

In the hypothetical involving the healthcare software company, imagine if an authentication flaw in a third-party AI's API allowed a hacker group to intercept the data stream, exposing thousands of medical images and associated protected health information (PHI). Claims of HIPAA/GDPR/CCPA violations and potential multi-million-dollar penalties from regulators are on the horizon. Even if an AI provider like Microsoft takes responsibility for the specific vulnerability, the healthcare software provider could still face liability on the basis that the healthcare company has a heightened duty to secure personal data through adequate vetting of third-party partners and end-to-end encryption. *See e.g., In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 1010–11 (N.D. Cal. 2016) (finding the plaintiffs could pursue breach of contract claims as third-party beneficiaries because the contract terms established that the defendant "could be held to privacy standards above and beyond the standards required under federal law"). If the operative service contract with the software vendor includes a clause representing that the software vendor will follow "industry best practices" for safeguarding PHI, this could impose further liability on a software vendor in this scenario.

IP CONSIDERATIONS

Beyond errors and security risks, software that relies on third-party AI also introduces potential complexities associated with protecting intellectual property rights. For example, poorly worded software license agreements may leave ambiguity over ownership rights to the AI model’s inputs and the outputs they generate.

Scenarios where copyrighted works are used to train AI LLMs to allegedly create infringing derivative works are already the subject of contentious litigation. *See, e.g., Kadrey and Silverman et al. v. Meta Platforms, Inc.*, 3:23-cv-03417 (N.D. Cal., July 7, 2023) (plaintiffs allege that LLaMA’s “outputs (or portions of the outputs) are similar enough to the plaintiffs’ books to be infringing derivative works”). Considering the healthcare software company scenario described earlier, imagine that the licensed software utilizes AI services to generate data visualization charts and dashboards for medical service providers tailored to patient data. The AI provider could potentially exploit the software vendor’s proprietary code and the end customer’s confidential data to enhance its AI model for competitors of the software vendors and end customer. The AI provider might also assert intellectual property rights over outputs generated by the AI services, even when those outputs are derived using software vendor code and end customer data inputs. This could have a substantial impact on the software provider’s leverage in the competitive marketplace, and increases the possibility that confidential customer information is used without permission.

Infringement liability is also an important consideration. If the AI service is found to have infringed third-party IP rights through techniques like training-data scraping, the software vendor could be liable for resulting copyright violations.

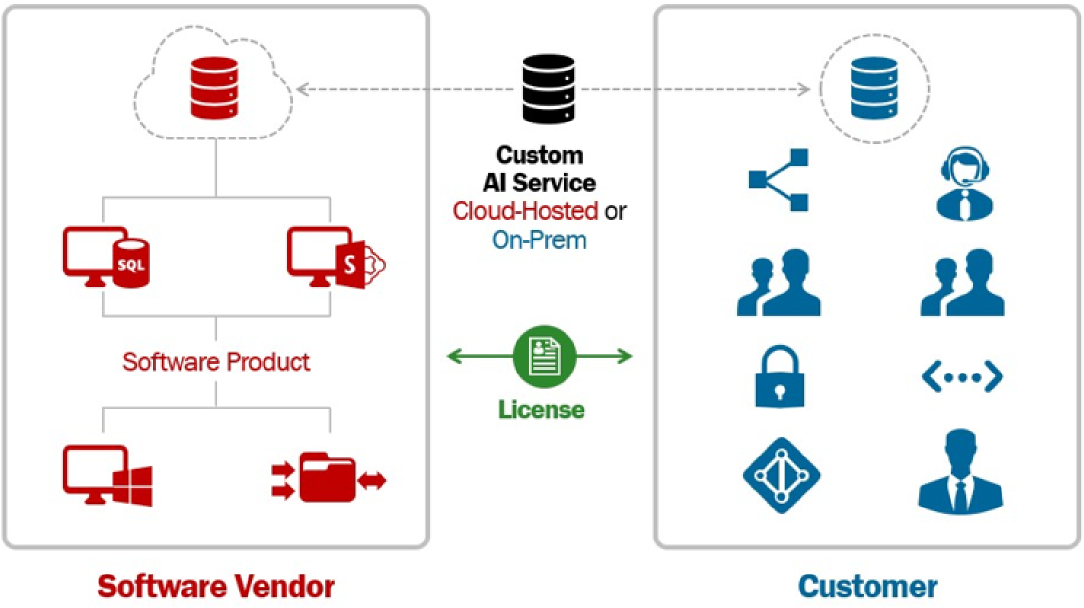
AI provider terms and conditions regarding IP rights vary. For example, Anthropic lets its users “retain all right, title, and interest—including any intellectual property rights” in the input or the prompts. In addition, Anthropic disclaims rights to customer content and states that customers own all outputs generated, assigning any potential rights in outputs to the customer. However, Anthropic’s commitment not to train its models on customer content explicitly mentions only “Customer Content from paid Services” and is subject to customers’ compliance with Anthropic’s terms of service. See ANTHROPIC’ S TERMS OF SERVICES, https://www.anthropic.com/legal/commercial-terms. Parties leveraging AI need to carefully consider implications relating to IP rights.

Beyond errors and security risks, software that relies on third-party AI also introduces potential complexities associated with protecting intellectual property rights.

SOFTWARE PRODUCTS THAT LEVERAGE CUSTOM-BUILT AI, EITHER ON-PREMISES OR IN THE CLOUD

Software products that rely on proprietary AI solutions deployed on-premises or in the software provider's cloud can allow for increased flexibility and control over features, as well as greater control over access to confidential data. At the same time, the party responsible for providing and maintaining the underlying infrastructure that houses the AI services faces heightened risks relating to data governance, system integration, and product/service quality.

The following figure illustrates a scenario where a Customer licenses software that leverages custom-built AI functionality hosted either (1) on premises on Customer IT infrastructure or (2) in the cloud by the software vendor.



In the above scenario, the services responsible for providing AI functionality reside either in the Customer's or the Software Vendor's IT infrastructure. The location where the AI services reside is important, as the entity responsible for managing that infrastructure may incur "gatekeeping" responsibilities tied to the use of the AI service. This gatekeeping duty can carry significant liability risks. The arrangement and location of the AI functionality also raises important questions regarding performance guarantees.

GATEKEEPER ROLE

Assume Software Vendor sells expense management software that uses custom-tailored NLP AI hosted on the Software Vendor's cloud to scan invoices and automate payments. The NLP AI model ultimately misinterprets handwritten figures, causing a client to overpay a vendor by $5 million. While the Software Vendor could argue that their NLP API simply passed along raw outputs and it was the Customer's responsibility to scrutinize those outputs before acting on them, a court could find that a "decision aid" technology vendor has a duty to implement appropriate safeguards and human oversight checkpoints. The fact that the AI services are hosted on the Software Vendor's cloud heightens the risk of this potential outcome.

As another example, assume Software Vendor sells automated hiring and resume screening software that leverages custom-built AI hosted on-premises in the Customer's IT infrastructure. This kind of tool should be designed to prevent illegal discrimination and bias from impacting hiring decisions. *See Mobley v. Workday Inc.*, No. 3:23-cv-00770 (N.D. Cal, Feb. 21, 2023) (EEOC filed suit against human resources software firm Workday alleging that it violated federal anti-bias laws by using AI-powered software to screen out job applicants for racially discriminatory reasons). The Customer in this scenario needs to consider the risks associated with hosting and relying on automated software that leverages AI—which has known issues tied to generating responses that exhibit bias and errors. Customers utilizing such AI solutions should consider dedicated human oversight teams reviewing outputs for compliance with ethical guidelines.

Finally, assume Software Vendor sells software solutions to FinTech companies that use AI to detect financial crimes, payment fraud, and identity theft. The Customer—and potentially the Software Vendor, depending on the nature of the license agreement—may have a gatekeeping duty to validate AI outputs and correct false positives that stem from any racial or religious biases before freezing accounts or reporting individuals to authorities.

SERVICE LEVEL AGREEMENTS (SLAS) AND PERFORMANCE GUARANTEES

The transient, evolving nature of AI requires a more nuanced approach to uptime guarantees commonly included in service level agreements. Consider, for example, Software Vendor sells AI-powered software that monitors data centers, dynamically detects anomalies, and predicts system failures. Certain AI systems are susceptible to natural performance degradations over time that occur as real-world data distributions shift, deviating from those on which the static AI model was initially trained. If the Software Vendor provides guarantees for software uptime—commonly included in a service-level agreement—degradations on software performance caused by changes in third-party AI models could violate software uptime promises. In a potential legal dispute over breach of a service level agreement with uptime requirements, a court might conclude that for a product that touts AI as a key selling point over traditional algorithms, the AI-powered product must remain continually tuned and calibrated to maintain a reasonable level of predictive or analytical performance. For traditional software, uptime means computational availability, but for AI solutions, “uptime” might need to account for the availability of accurate, effective outputs from the AI models themselves.

LESSONS LEARNED FROM LITIGATION—BEST PRACTICES

Software that leverages AI functionality often handles personal information, financial data, intellectual property, and other sensitive information. This raises important liability considerations for software vendors and companies that license AI-powered software. The following list offers some best practices for parties seeking to proactively manage risks when writing and negotiating software license agreements:

FOR SOFTWARE PRODUCTS THAT USE THIRD-PARTY AI

1. Carefully scrutinize broad “as is” clauses for third-party components, as they may offer less protection than anticipated.
2. Rigorously test any AI service before integration—and document these efforts.
3. Negotiate stronger indemnification terms with third-party AI service providers, especially for enterprise clients.
4. Identify and provide notice of functions that rely on external AI services, and clearly articulate limitations on capabilities.
5. Clearly articulate IP ownership rights associated with AI-generated content, including ownership of inputs and outputs, as well as rights associated with trained AI models and use across different deployment environments.
6. Regularly audit third-party AI performance, and provide customers with direct links to the third party’s performance metrics and incident reports.
7. Ensure that any marketing materials accurately describe AI-related capabilities and limitations.
8. Memorialize procedures for secure data storage, retention periods, and deletion processes.
9. Ensure the AI system’s data practices adhere to data privacy laws like GDPR and CCPA, and update these practices as more jurisdictions put new laws in place.

FOR SOFTWARE PRODUCTS THAT USE CUSTOM-BUILT AI

10. Articulate whether AI software is hosted on-premises on Customer IT infrastructure or in the cloud by the software vendor, and detail responsibilities for data protection, security, and performance.

11. Explicitly outline the scope of any gatekeeping responsibility over AI solutions to comply with legal and ethical requirements.

12. Establish concrete metrics for "reasonable AI performance" that align with the parties' expectations as well as known issues with AI performance, such as training data drift.

While the evolving capabilities of AI bring increased functionality and features, they also raise important legal considerations for parties negotiating software license agreements. As software incorporating AI becomes more common, disputes over software license terms are likely to increase. Software vendors and licensees alike should understand and carefully consider the risks associated with licensing AI software. Those unwilling to embrace this responsibility could face significant business and legal repercussions as the "move fast and break things" ethos collides with the general public's demands for safe, reliable, accountable, and ethical use of AI.

BRYAN MECHELL

Bryan Mechell is a trial lawyer and registered patent attorney with experience in complex intellectual property litigation. Bryan focuses his practice on new and cutting-edge technologies in order to help large companies, small businesses, and inventors assess and protect the value of their IP.

LinkedIn | Connect with Bryan!

NAVIN RAMALINGAM

Navin Ramalingam is an attorney specializing in intellectual property and technology litigation. He helps inventors, entrepreneurs, and businesses protect and monetize their intellectual property by leveraging his strong business acumen and lifelong passion for technology and innovation.

LinkedIn | Connect with Navin!

AI'S IMPACT ON PROPERTY INSURANCE COVERAGE

BY LEE ANN THIGPEN

Artificial intelligence (AI) is the simulation of human intelligence processes by machines, such as computer systems for assistance in quickly answering complicated questions, researching a specific topic, or creating an image. Put another way, AI is the ability for computers to do tasks and solve problems that would otherwise require human intelligence, but to do those jobs faster and more efficiently.

In the insurance industry, AI can be applied to accelerate underwriting and claims processes, to offer more personalized, targeted coverage by analyzing available data on a particular risk, as well as detecting fraud and pro-actively work to prevent or mitigate losses.

AI is revolutionizing property insurance in a myriad of ways. Below this article will discuss several ways that AI is making an impact.

RISK ASSESSMENT/UNDERWRITING

Insurance underwriting involves assessing risks associated with insuring individuals or entities and determining the appropriate premiums and coverage. AI is increasingly being used in insurance underwriting to enhance accuracy, efficiency, and decision-making. The types of data available to insurers include information like previous claims and repair permit applications, but also crime statistics and aerial photography to provide an accurate, up-to-date assessment of hundreds of factors impacting risk and valuation. Vendors who offer proprietary tools to analyze both exterior and interiors of the home to provide information for rates and premium are an emerging field in the AI realm.

Here's how AI is transforming insurance underwriting:

- **Data Analysis:** AI algorithms can analyze vast amounts of data from diverse sources, including demographic information, claims history, credit scores, medical records, and even social media activity. By leveraging this data, insurers can gain deeper insights into the risk profile of applicants and make more informed underwriting decisions.
- **Predictive Modeling:** AI enables insurers to build sophisticated predictive models that assess the likelihood of future events, such as accidents, illnesses, or property damage. These models take into account various risk factors and help insurers estimate the probability and severity of potential losses.
- **Risk Segmentation:** AI allows insurers to segment their risk pool more effectively by identifying subgroups of policyholders with similar risk profiles. This enables insurers to tailor their underwriting criteria, pricing strategies, and coverage options to better meet the needs of different customer segments.
- **Automated Underwriting:** AI-powered underwriting platforms can automate the underwriting process for standard or low-risk applications, speeding up decision-making and reducing the need for manual intervention. This frees up underwriters to focus on more complex cases that require human judgment.
- **Real-time Risk Assessment:** AI enables insurers to continuously monitor and update risk assessments in real-time based on changing circumstances, such as changes in market conditions, regulatory environment, or customer behavior. This allows insurers to adapt their underwriting strategies dynamically and mitigate emerging risks proactively.
- **Natural Language Processing (NLP):** NLP technology allows insurers to extract valuable insights from unstructured text data, such as medical reports, claim forms, and customer communications. This helps underwriters make more informed decisions by analyzing relevant information more efficiently.

- **Personalized Underwriting:** AI enables insurers to offer more personalized underwriting decisions and pricing based on individual risk factors, preferences, and behaviors. This enhances the customer experience and improves customer satisfaction and retention.

CLAIMS PROCESSING: AI algorithms can automate claims processing by analyzing photos, videos, and other documentation submitted by policyholders to assess damages and determine payouts. This speeds up the claims process and reduces the need for manual intervention. Insurance claim processing using AI involves leveraging AI and machine learning algorithms to streamline and improve various aspects of the claims management process.

Below is an overview of how AI is typically used in insurance claim processing:

- **Automated Document Processing:** AI-powered optical character recognition (OCR) technology can automatically extract relevant information from various documents, such as claim forms, invoices, police reports, and medical records. This helps in reducing manual data entry errors and accelerates the processing time.

- **Fraud Detection:** AI algorithms can analyze historical data and patterns to identify potentially fraudulent claims. By flagging suspicious claims early in the process, insurers can investigate further and prevent fraudulent payouts, saving both time and money.

- **Predictive Analytics:** AI models can analyze vast amounts of data to predict claim outcomes, such as the likelihood of a claim being approved or denied, the expected cost of the claim, and the optimal settlement amount. This helps insurers make more informed decisions and allocate resources effectively.

AI algorithms can automate claims processing by analyzing photos, videos, and other documentation submitted by policyholders to assess damages and determine payouts.

- **Image and Video Analysis:** AI-powered computer vision technology can analyze images and videos submitted as part of the claim to assess damage, estimate repair costs, and verify the authenticity of the claim. This is particularly useful for property and auto insurance claims.

- **Customer Service Chatbots:** AI-powered chatbots can assist policyholders throughout the claims process by answering common questions, providing status updates, and guiding them through the necessary steps. This improves customer satisfaction and reduces the workload on human agents.

- **Natural Language Processing (NLP):** NLP algorithms can analyze unstructured text data from emails, social media, and customer feedback to extract valuable insights and sentiment analysis. This helps insurers better understand customer needs and preferences, leading to more personalized service.

- **Process Automation:** AI can automate repetitive tasks and workflows within the claims processing cycle, such as routing claims to the appropriate department, sending notifications to stakeholders, and updating internal databases. This increases efficiency and frees up human resources to focus on more complex tasks.

- **Continuous Learning and Improvement:** AI systems can continuously learn from new data and feedback to improve their performance over time. By iteratively refining their models and algorithms, insurers can stay ahead of emerging trends and adapt to changing market dynamics.

FRAUD DETECTION: AI algorithms can detect patterns indicative of fraudulent claims, such as inconsistencies in reported damages or suspicious behavior. This helps insurance companies prevent fraud, saving them significant amounts of money. Insurance fraud costs US consumers more than $80 billion annually. This results in the average American family paying hundreds of additional dollars in premiums each year. An accurate, up-to-date understanding of property condition can also be useful in countering fraudulent claims. This is important given the rising use of “deep fakes,” which are images or videos that have been doctored or created by using AI in attempt to fool those viewing the images.

Here are a few ways that AI is applied in fraud prevention in insurance claims:

- **Anomaly Detection:** AI algorithms can analyze vast amounts of historical claims data to identify patterns and anomalies indicative of potential fraud. By comparing new claims to established patterns, AI systems can flag suspicious claims for further investigation.

- **Predictive Modeling:** AI enables insurers to build predictive models that assess the likelihood of a claim being fraudulent based on various risk factors, such as claimant demographics, past claim history, and behavioral patterns. These models help insurers prioritize claims for review and allocate resources more effectively.

- **Pattern Recognition:** AI-powered systems can recognize common patterns and techniques used in fraudulent claims, such as staged accidents, inflated medical bills, or false documentation. By continuously learning from new data, AI systems can adapt to evolving fraud schemes and improve detection accuracy over time.

- **Social Network Analysis:** AI algorithms can analyze social networks and relationships between claimants, service providers, and other relevant entities to uncover potential collusion or organized fraud rings. By mapping out these connections, insurers can identify suspicious networks and investigate accordingly.

- **Text Mining and Natural Language Processing (NLP):** AI technologies such as NLP can analyze unstructured text data from claim forms, medical records, police reports, and other documents to extract valuable insights and detect inconsistencies or red flags indicative of fraud.

- **Image and Video Analysis:** AI-powered computer vision technology can analyze images and videos submitted as part of the claim to assess damage, verify the authenticity of documentation, and identify signs of tampering or manipulation.

- **Real-time Monitoring:** AI enables insurers to monitor claims in real-time and detect fraud as it occurs. By setting up alerts and triggers based on predefined criteria, insurers can intervene promptly to prevent fraudulent payouts.

- **Collaborative Intelligence:** AI facilitates collaboration between insurers, law enforcement agencies, and other stakeholders in the fight against insurance fraud. By sharing data and insights, industry players can better identify fraud trends, share best practices, and coordinate efforts to combat fraud more effectively.

LOSS PREVENTION: Loss prevention in insurance claims involves implementing strategies to minimize the occurrence and severity of losses covered by insurance policies. Artificial intelligence (AI) is increasingly utilized to enhance loss prevention efforts in insurance claims.

Here's how AI is applied in this context:

- **Risk Assessment:** AI algorithms can analyze vast amounts of data to assess the risk associated with insuring individuals, properties, or businesses. By leveraging data from various sources, including historical claims data, demographic information, and external risk factors, AI systems can identify high-risk entities and help insurers take proactive measures to mitigate potential losses.
- **Predictive Analytics:** AI enables insurers to build predictive models that forecast the likelihood and severity of future losses based on historical data and relevant risk factors. These models help insurers identify emerging trends, anticipate potential risks, and implement preventive measures to reduce the frequency and impact of losses.
- **Real-time Monitoring:** AI-powered systems can monitor events and activities in real-time to detect potential risks or anomalies that may lead to losses. For example, AI can analyze sensor data from IoT devices to detect fire, theft, or other hazards in insured properties and trigger alerts for immediate action.
- **Fraud Detection:** While we've discussed fraud detection separately, it's worth noting that AI can also contribute to loss prevention by detecting fraudulent activities that could lead to financial losses for insurers. By identifying and preventing fraudulent claims, insurers can mitigate their overall losses and maintain the integrity of their operations.
- **Safety and Security Solutions:** AI technologies such as computer vision, natural language processing, and machine learning can be applied to develop safety and security solutions that help prevent losses in various contexts. For example, AI-powered surveillance systems can monitor traffic patterns to prevent accidents, analyze security footage to deter theft, or identify potential hazards in industrial settings to prevent workplace injuries.

Loss prevention in insurance claims involves implementing strategies to minimize the occurrence and severity of losses covered by insurance policies.

- **Personalized Risk Management:** AI enables insurers to offer personalized risk management solutions tailored to the specific needs and characteristics of individual policyholders. By analyzing data on customer behavior, preferences, and risk factors, insurers can recommend proactive measures and risk mitigation strategies to help policyholders reduce their exposure to losses.

- **Claims Analytics:** AI-powered claims analytics platforms can analyze claims data to identify patterns and root causes of losses, allowing insurers to implement targeted interventions to prevent similar losses in the future. By understanding the underlying drivers of losses, insurers can develop more effective loss prevention strategies and improve overall risk management practices.

CUSTOMER SERVICE: AI is revolutionizing customer service in insurance claims by offering more efficient, personalized, and accessible assistance to policyholders throughout the claims process. Here's how AI is beginning to change the landscape of customer service in insurance claims:

- **24/7 Availability:** AI-powered chatbots and virtual assistants provide round-the-clock support to policyholders, allowing them to report claims, check claim status, and get answers to common questions anytime, anywhere. This ensures that customers can access assistance whenever they need it, without being limited by traditional business hours.

- **Instant Responses:** AI-powered chatbots can provide instant responses to customer inquiries, significantly reducing wait times and improving overall responsiveness. Customers no longer have to wait on hold or wait for a response to an email—they can get the information they need instantly through AI-driven chat interfaces.

- **Efficient Claim Reporting:** AI-enabled virtual assistants guide policyholders through the claim reporting process, asking relevant questions and collecting necessary information in a structured and efficient manner. This reduces the likelihood of errors and omissions in claim submissions, leading to faster processing times and smoother claim resolution.

- **Personalized Assistance**: AI algorithms analyze customer data and interaction history to personalize the customer service experience. By understanding each customer's preferences, needs, and past interactions, AI-driven systems can tailor responses and recommendations to provide more relevant and helpful assistance.

- **Claims Status Updates:** AI-powered systems can provide real-time updates on claim status and progress, keeping policyholders informed throughout the claims process. This reduces uncertainty and anxiety for customers and improves transparency and trust in the insurance company.
- **Proactive Communication:** AI can analyze data to identify situations where proactive communication with customers may be beneficial, such as sending reminders about policy renewals, offering tips for risk mitigation, or providing updates on relevant industry trends. This proactive approach helps insurers build stronger relationships with customers and enhance overall satisfaction.
- **Claims Triage and Routing:** AI algorithms can triage incoming claims and route them to the appropriate department or adjuster based on factors such as severity, complexity, and urgency. This ensures that claims are handled promptly and efficiently, optimizing resource allocation and improving customer service levels.
- **Natural Language Processing (NLP):** NLP technology allows AI systems to understand and process natural language input from customers, enabling more natural and intuitive interactions. Customers can communicate with AI-driven chatbots using their own words and receive accurate and relevant responses, enhancing the overall customer service experience.

AI has already begun to transform the insurance industry and shape best practices, resulting in more efficient processes, better products for consumers, and more informed claims handling. As this technology continues to be refined, the industry will continue to adapt and make use of these new tools.

LEE ANN THIGPEN

Lee Ann Thigpen is an experienced litigator with over 20 years of experience serving clients both nationwide and internationally in complex insurance coverage disputes. Her practice focuses primarily on representing insurers and reinsurers in construction and energy-related industries.

LinkedIn | Connect with Lee Ann!

FRONT AND CENTER

PHILIP SIEFF

TARA SUTTON

MICHAEL REIF

RASHANDA BRUCE

JULIE REYNOLDS

ROBINS KAPLAN SECURES $7.75 MILLION VERDICT IN AEROSOL DUST REMOVER ABUSE CASE

Robins Kaplan secured a significant $7.75 million verdict against CRC Industries for failing to prevent the foreseeable misuse of its aerosol dust remover products. This case, the first of its kind to go to trial, arose from the tragic death of Cynthia McDougall, who was killed in a vehicle crash caused by an individual impaired from huffing CRC Duster. The verdict emphasizes the responsibility of manufacturers to prevent the misuse of their products, particularly when the dangers are well-known. While the jury did not award punitive damages, they urged CRC Industries to lead efforts in addressing inhalant abuse within their industry. The trial team was led by Tara Sutton and Philip Sieff and included attorneys Michael Reif, Rashanda Bruce, and Julie Reynolds.

AWARDS + RECOGNITIONS

LOGAN DREW

CHRISTOPHER LARUS

ROBINS KAPLAN APPOINTS NEW LEADERSHIP FOR NATIONAL INTELLECTUAL PROPERTY & TECHNOLOGY AND TRIAL GROUPS

Logan Drew has been named Chair of the firm’s National Intellectual Property and Technology (IP&T) Litigation Group. Drew succeeds Christopher Larus, who will now serve as National Trial Chair alongside Roman Silberfeld to lead the firm’s trial practice.

“These leadership changes represent an exciting new chapter for our firm,” said Anthony Froio, Chair of the Executive Board and Managing Partner at Robins Kaplan. “I’m confident that Logan and Chris will excel in their new roles, advancing our strategic goals and ensuring continued success for our clients.”

CHAMBERS USA RECOGNIZES 5 ROBINS KAPLAN PRACTICE GROUPS AND 21 LAWYERS IN 2024 GUIDE

Noted for their sophisticated, high-impact work, Robins Kaplan practice groups have been ranked in the *Chambers USA Guide 2024* in the following categories and geographies:

- Antitrust – Nationwide: Plaintiff (Band 1)
- Antitrust – New York: Mainly Plaintiff (Band 1)
- Antitrust – Minnesota (Band 1)
- Insurance – Massachusetts (Band 3)
- Insurance: Insurer - California (Band 4)
- Intellectual Property – Minnesota (Band 1)
- Litigation: General Commercial – Minnesota (Band 1)
- Litigation: General Commercial – South Dakota (Band 2)
- Native American Law – Nationwide (Band 2)

THE AMERICAN LAWYER RANKS ROBINS KAPLAN AMONG TOP 15 FIRMS IN NATION FOR *PRO BONO* WORK IN 2024

Robins Kaplan has been ranked among the top 15 firms in the nation for *pro bono* work according to *The American Lawyer*'s annual *pro bono* survey, which highlights the AmLaw 200 firms with the deepest commitment to *pro bono* work. In 2023, Robins Kaplan provided over 19,500 hours of *pro bono* service in partnership with over 60 nonprofit organizations.

STEVE SCHUMEISTER HONORED WITH TWIN CITIES DIVERSITY IN PRACTICE DISTINGUISHED SERVICE AWARD

Steve Schumeister has been recognized with the Twin Cities Diversity in Practice (TCDIP) Distinguished Service Award. TCDIP is a nonprofit association of more than 70 law firms and corporate legal departments, and this is only the second time this prestigious accolade has been awarded in TCDIP's 19-year history.

STEVE SCHUMEISTER

ROBINS KAPLAN NAMED TO 2024 BTI CLIENT SERVICE A-TEAM

Robins Kaplan has been named to BTI Consulting's 2024 Client Service A-Team, recognizing law firms that provide elite client service. The BTI Client Service A-Team report stands out as the sole law firm ranking derived from direct input from top legal decision-makers at many of the world's largest organizations. The research, gathered in BTI's Annual Survey of General Counsel, maintains its independence and impartiality, with sponsorship limited solely to BTI.

FEATURED APPELLATE RESULTS

U.S. SUPREME COURT VACATES LOWER COURT RULING IN STATE LEGISLATIVE MAP DISPUTE

Robins Kaplan, along with the Native American Rights Fund, Campaign Legal Center and the Law Offices of Bryan Sells, represents the Turtle Mountain Band of Chippewa Indians and Spirit Lake Tribe in a Voting Rights Act dispute filed in February of 2022. This dispute arose from a North Dakota legislative redistricting plan that the tribes alleged had an effect of diluting the votes of Native Americans living in north-central North Dakota. During discovery, plaintiffs served subpoenas on current and former North Dakota lawmakers and the lawmakers moved the District Court to quash those subpoenas. The district court denied these motions and the defendants appealed the ruling to the Eight Circuit Court of Appeals, which reversed the ruling and directed the lower court to quash all but one subpoena. While the discovery dispute was being litigated in the appellate court, the Tribes prevailed in District Court and the North Dakota State Legislature was ordered to adopt a new plan that would remedy Voting Rights Act violations.

The tribes then petitioned the Supreme Court to take up the discovery matter. The Petition to the Supreme Court presented two questions: (1) Should the Court vacate the Eighth Circuit's decision? (2) Are state legislatures absolutely immune from civil discovery or is the state legislative privilege a qualified one that yields where important federal interest are a stake? The Supreme Court ruled in favor of the Petitioners, granting cert and the motion to vacate the judgment. In August 2024, the Eighth Circuit issued a judgment dismissing the case as moot.

VICTORY FOR COMMERCIAL INSURANCE COMPANY IN COVID-19 POLICY COVERAGE DISPUTE

In July 2024, the U.S. Court of Appeals for the 2nd Circuit affirmed the District Court of Connecticut's judgment in favor of Factory Mutual Insurance Company in a Covid-19 pandemic-related insurance coverage dispute. The case centered around whether Amphenol Corporation's claimed economic losses due to the COVID-19 pandemic were covered under its first party property insurance policy issued by FMIC.

Amphenol Corporation, a manufacturer and distributor of electronic components, filed a complaint against Factory Mutual in January of 2021. Amphenol alleged $100 million in property damage and business interruption losses due to "physical loss or damage" caused by the Covid-19 virus. Amphenol sought to amend its complaint to include proposed allegations that the virus "adsorbed" or "attached" to property, remained infectious for up to a month, and that Amphenol engaged in substantial "repair or remediation efforts" to address the alleged adsorption or attachment of the virus. The District Court denied the motion to amend and issued judgment on the pleadings in favor of FMIC.