When algorithms go to court: the new frontier of AI liability and litigation in the U.S.

A Case Study into litigation and liability associated with Artificial Intelligence in the United States of America.

AI Liability and Enforcement

How existing U.S. Laws and government agencies are impacting AI development and implementation.

This article explores how the United States government is already regulating the field of artificial intelligence (AI), even without a specific AI regulation. You will see how regulatory bodies and enforcement agencies are utilizing existing legislation to hold companies developing and deploying AI-enabled technology accountable for bad outcomes.

These government organizations are applying the law in novel ways, while generally staying in line with the legislator’s initial purpose. Finally, we will explore how organizations can mitigate legislative risks and maximize AI performance in order to accelerate the adoption of AI-enabled systems.

The rise of AI liability

The digital age has put enormous pressure on regulators, as new digital technologies are accessible worldwide almost from the moment they are first deployed.

AI (particularly large language models (LLMs)) such as ChatGPT, Claude, Gemini is just the latest example of rapid development and even faster deployment and adoption. To make things even more problematic, some of the most critical and sensitive sectors are among the first to implement AI into their workflows, including finance, communications, hiring, security, and surveillance.

While the growing market is a massive opportunity for companies developing and deploying AI vision and computer vision systems, it also carries unique risks that can have far-reaching consequences. Repercussions that can directly impact both businesses and end users or consumers such as biases, misidentification, false alerts, discrimination, and other problems associated with lack of transparency. While worldwide legislators have already addressed the rise of AI with separate laws, such as the EU's AI Act, the United States has yet to implement dedicated Federal AI regulations.

This does not mean AI isn't regulated in the U.S., on the contrary. Authorities, such as the Federal Trade Commission (FTC) and Department of Justice (DOJ) are finding innovative ways to leverage existing laws and expand their scope to hold companies accountable for AI-related harms.

Most AI-related litigation is ongoing so legal precedent is still evolving and as such, companies may be at risk of being swept into the growing wave of lawsuits, investigations, and reputational fallout for how AI is built, deployed and used.

As a result, the development and use of AI carry significant enforcement and litigation risks.

Supporting references

1 Copyright – CMS AI and Copyright Case Tracker, Map of AI Copyright Lawsuits and AI Lawsuits Connections
2 Privacy – The Stanford 2025 AI Index Report noted a 56.4% increase in AI-related incidents, including privacy violations and data leaks, in 2024 alone.
3 Discrimination – AI Equality, Bias and AI Discrimination Case Tracker

How the U.S. regulates AI without an AI-specific law

As you will soon see, the existing U.S. legislature has a significant impact on AI, both in terms of development and deployment. To help you understand how, BSI have created this list that provides a bird's-eye view of the current regulations, particularly from an agency-to-agency perspective.

However, be aware that there's an incredible amount of legal uncertainty at present. Not only is technology rapidly advancing, but regulators are also adapting in real-time, broadening the scope of existing regulations. And they are doing it with a stick, as evidenced by the latest FTC AI crackdowns. In other words, the burden of that legal uncertainty falls on the AI developers and companies who are looking to implement AI solutions.

Agency-by-agency case examples

Here's how agencies are approaching AI and finding creative ways to interpret existing laws for new technologies:

Federal Trade Commission (FTC)

The Federal Trade Commission Act, as the primary statute of the FTC, also serves to enforce against AI misuse, primarily through legal institutions of unfair or deceptive practices.

In particular, FTC is focusing on "AI washing" malpractices affecting the marketplace. AI washing is a practice of inflating claims of AI capabilities to mislead users. DoNotPay is a prime example of this, as the company advertised "robot lawyers," but in reality, the service was neither robotic nor automatic, and it could not substitute for expert legal advice.

The primary takeaway for AI companies regarding FTC compliance primarily pertains to marketing, emphasizing the importance of transparency when making promises to potential customers and clients.

Agency-by-agency case examples

Securities and Exchange Commission (SEC)

The SEC enforces the Securities Exchange Act, a nearly 100-year-old law that remains in effect. The SEC's primary role is to monitor and ensure accurate and timely disclosures in the securities industry. Due to the significance of speed, alongside fast and accurate data processing in the securities industry, AI and financial companies have rushed to enter the market, offering AI-powered solutions to help speed up decision making.

However, this has drawn the SEC's attention, and they have already held public meetings to discuss the use of AI. The primary concern is the accuracy and reliability of AI-powered disclosures. Just like other agencies and authorities, the SEC is also interested in preventing AI washing and determining if companies are overstating their AI claims to attract investors to their products.

Considering the value of the securities market and the importance of the industry as a whole, companies looking to develop or deploy AI solutions in this field should be additionally careful, as higher rewards often carry higher risks.

Food and Drug Administration (FDA)

Although it may not be immediately apparent, the FDA regulates AI as a "software as a medical device" under the Federal Food, Drug, and Cosmetic Act (FD&C Act). The FDA primarily focuses on safety and efficacy failures, as well as specific cases of AI washing, regarding the misleading promotion of AI health products.

As a prominent example, the FDA sent a warning letter to Exer Labs, Inc., notifying them of their unsupported claims regarding their AI-based products, which were made without proper approvals and proof of the claimed benefits.

Equal Employment Opportunity Commission (EEOC)

The hiring and recruitment industry was one of the first to welcome AI capabilities, primarily for resume parsing. However, this practice is closely monitored by the EEOC, as it can easily result in discrimination and similar unwelcome employment practices.

The EEOC enforces several statutes relating to work and employment, most notably the Civil Rights Act and the Americans with Disabilities Act (ADA), both of which explicitly prohibit employment discrimination. Due to the widespread use of AI in hiring, several litigation cases have already been filed in the U.S.

One of the most high-profile litigation cases is the ongoing Workday lawsuit, where it is alleged that this popular HR software, which utilizes computer vision in its assessments, exhibits bias in its automated decision-making.

The developments underscore the EEOC emphasis on the fair and transparent use of AI, particularly in sensitive decisions such as hiring and promotions, where discrimination is strictly prohibited.

Agency-by-agency case examples

Federal Communications Commission (FCC)

The Communications Act of 1934 and the Telecommunications Act of 1996 grant the FCC a broad enforcement scope that encompasses the use of AI.

In particular, the FCC regulates the use of AI in the communications infrastructure, which includes computer vision tools such as surveillance cameras, IoT devices, and similar platforms.

Computer vision systems pose privacy and cybersecurity risks, including breaches, as well as the transmission of biometric data over telecom networks without consent and proper safeguards. The FCC closely monitors AI use, and we have even seen election interference cases involving AI technology, which is why companies must be particularly vigilant with compliance.

Health and Human Services, Office for Civil Rights (HHS OCR) / HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) and particularly its privacy and security rules are enforced by HHS OCR. In terms of AI, the HHS OCR governs Protected Health Information (PHI), as it contains highly sensitive personal data regarding individuals' health.

The risks associated with this type of data are enormous, particularly when it comes to chatbots, as well as cloud-based vision tools and image analysis. It's imperative to process and store fragile health-related data with proper safeguards. Businesses must ensure that they have signed Business Associate Agreements (BAAs) that guarantee their partners maintain HIPAA standards, particularly when working with third-party service providers that may come into contact with sensitive personal data.

As noted, the risks are omnipresent, as users themselves sometimes upload their most private information without knowing the exact way the data is collected (and shared). Therefore, signing impeccable B2B contracts with partners and having clear privacy policies for users help ensure you avoid hefty HIPAA fines and potential costs related to lengthy proceedings.

Department of Homeland Security (DHS) / Customs and Border Protection (CBP)

The Immigration and Nationality Act and Homeland Security Act allow the DHS and CBP a broad spectrum of monitoring and regulating activities. They themselves use AI-powered facial recognition and biometric systems.

Because these activities carry an extraordinarily elevated risk of bias and privacy, both DHS and CBP are authorized to investigate vendors and impose restrictions.

Therefore, companies that provide AI and computer vision solutions for border control purposes must ensure their systems don't create discriminatory impacts and are also in line with the highest privacy and security standards.

Key themes across AI litigation

While AI use is broad, and generalizations are rarely welcome in the legal field, some patterns are noticeable in AI litigation, as well as in the approaches government agencies take when interpreting the existing laws and statutes to the latest tech.

Sector-specific, but expanding liability

While healthcare, finance, media, and publishing are leading the way, agencies in other sectors are quickly catching up.

Computer vision AI enforcement is gaining significance in sectors such as HR (automated screening and parsing), surveillance, and security (biometric authentication), as well as manufacturing and retail analytics.

As such, the agencies enforcing the rules in each sector are quickly catching up and expanding the scope of their governing statutes to AI use, even without a distinct law.

Common risks across domains

We can see some common themes in agency enforcement and litigation:

AI washing: Businesses making deceptive claims about their AI features are facing scrutiny, as most agencies are monitoring deceptive claims.

Lack of transparency: AI companies are required to publicly disclose the limitations of their software, specifically any potential biases in vision algorithms, error rates, and data sharing policies.

Algorithmic bias: AI companies find it hard to maintain bias-free and accurate results. Any discrimination or prejudice may result in costly fines and lengthy litigation.

Data misuse and privacy issues: Following (international) privacy standards is never easy. Still, things get even more complicated when AI is involved, and especially when collecting and sharing biometric data and protected health information (PHI).

Legal uncertainty and overlapping jurisdictions

Since there’s no unified federal AI law, companies are required to comply with multiple authorities simultaneously. This places tremendous burdens on the compliance and legal departments, as they must comply with various national agencies and also with international legislation, such as the EU’s AI Act and GDPR.

For example, suppose a company is developing an HR tool. In that case, it may face scrutiny by the FTC for deceptive marketing, the EEOC for any biases in decision-making, and privacy authorities under the HIPAA Act, as well as internationally, due to GDPR.

Proactive compliance as a differentiator

However, organizations that invest in AI algorithmic auditing, data testing, and acquiring reputable third-party certifications may gain a competitive edge. Not only can they avoid potential fines and reputational damage that follow, but they are also more likely to attract privacy-conscious clients and users who care about reputable companies using their sensitive information.

While it can be complicated, AI vision developers and deployers that follow universal principles, such as transparency, truthful marketing, demonstrable safety, and a privacy-first approach, have little reason to worry about agencies interfering with their work, let alone facing litigation.

Risk mitigation strategies for AI Vision and Computer Vision companies

While staying on top of different agencies and regulations might feel overwhelming, there are sound risk mitigation strategies AI vision companies can take to reduce litigation exposure and agency enforcement.

1 Third-party Model Testing

This Case Study has explored how computer vision applications may carry risk of bias, as well as other errors such as hallucination. Independent, third-party verification of model performance, robustness and fairness can provide substantive evidence of performance claims and risk mitigation when dealing with authorities. However, testing is not just a tick box activity: it may also reveal genuine flaws in your models or systems, allowing you to prevent further issues and genuinely improve your product.

2 Transparency and explainability reporting

Openly declaring the algorithm's decision logic and providing examples of how images are parsed, as well as which features have the most significant impact on the output, will help counter deceptive claims, and improve the perception of your company's ethical principles.

3 Testing, assessments, and certifications

Marketing and investor materials should emphasize independent testing, certifications, and other risk mitigation steps you have implemented into your AI model and systems lifecycle. That will not only raise the company's credibility but also serve as evidence in any potential enforcement situation, showing that you are committed to ethical and transparent AI throughout the product lifecycle including early design and development and post deployment monitoring.

4 Privacy and data protection safeguards

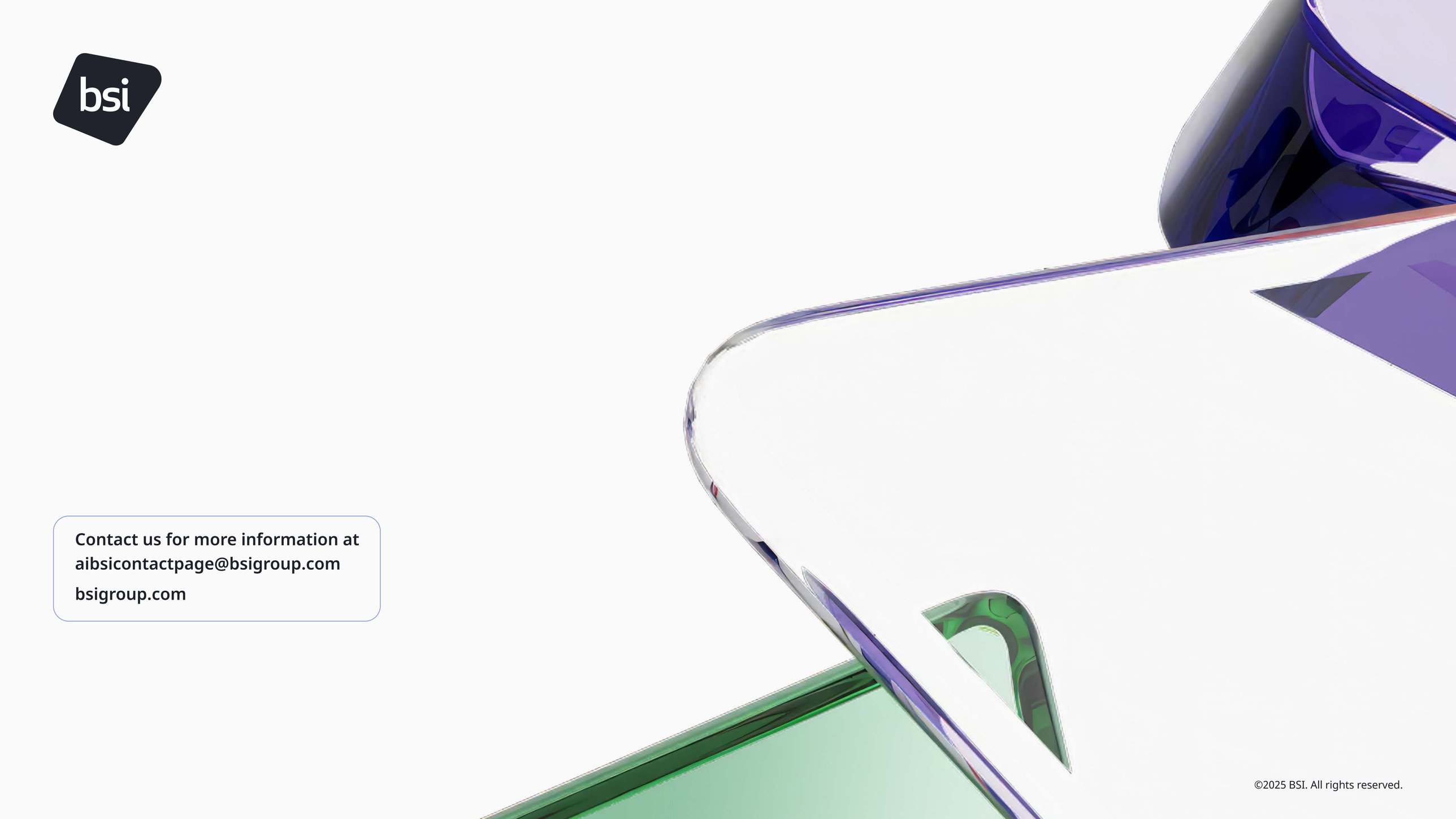
Privacy practices such as data minimization, anonymization, and encryption, all under sound Business Associate Agreements (BAA) and Data Processing Agreements (DPA), will ensure that your vendors and partners maintain the same level of security as you do. That will not only prevent enforcement action but can also serve as key evidence that you did your part as the data controller in case of any data breach or leakage.

Conclusion

This Case Study has explored an increasing trend in the number of AI litigation and enforcement cases across various types of law, including copyright, privacy, and discrimination. AI liability is on the rise despite the absence of federally enacted AI-specific law. The existing laws (even if 50 or 100 years old) have been proven to be sufficient for agencies to act and enforce the transparent, ethical and fair development and deployment of AI systems, which require careful and proactive compliance.

Companies developing, deploying and integrating AI vision technologies are under scrutiny, particularly if they operate in the health, HR, surveillance, or data analytics fields, as they may draw the attention of multiple agencies simultaneously. Because of the sensitive nature of the image data they process, companies in these fields are inherently high-risk, as any potential incorrect or biased decision-making and data breach can directly impact human lives. As such, AI vision systems require careful and proactive compliance.

Fortunately, measures such as independent, third-party assessments and model testing evidence risk management practices and AI performance, robustness and fairness enabling true transparency. Companies engaging in compliance activities can mitigate litigation risks and improve their systems to the benefit of the end user. Ultimately, making full legal compliance a natural consequence of quality and ethical AI development and implementation.



Contact us for more information at
aibsicontactpage@bsigroup.com

bsigroup.com