Legal 500
Country Comparative Guides 2024

United States
Artificial Intelligence

Contributor

Venable LLP

Justin Pierce

Partner | jepierce@venable.com

Eric Prager

Partner | eaprager@venable.com

Ryan Ward

Counsel | rtward@venable.com

Heather West

Senior Director of Cybersecurity and Privacy Services | hewest@venable.com

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in United States.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

United States: Artificial Intelligence

1. What are your countries legal definitions of "artificial intelligence"?

Artificial intelligence (AI) has been defined in 15 U.S.C. § 9401(3) as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action." This definition was a part of the National Artificial Intelligence Initiative Act of 2020 and has been used and referenced (sometimes with context-specific additions) in other proposals, laws, and executive orders since then, including the 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Apart from implementation of the National Artificial Intelligence Initiative Act (and other laws that expressly adopt this definition), the definition is not necessarily binding on courts or intellectual property offices like the U.S. Patent and Trademark Office. This definition is similar to the OECD definition that is often used in laws in other countries.

2. Has your country developed a national strategy for artificial intelligence?

The United States has developed several national strategies for AI, focusing on different aspects of the development, use, and regulation of AI.

- The most comprehensive is the 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, outlining over a hundred government actions for a society-wide effort that includes government, the private sector, academia, and civil society. Work to implement this EO, including on topic- or jurisdiction-specific strategies, has been rapidly advancing through the individual agencies. This includes creating AI standards, mitigating or preventing social harms, and fostering international cooperation and competition.
- The 2023 National Standards Strategy for Critical and Emerging Technology is intended to strengthen U.S. leadership and competitiveness in advanced technologies that are critical to the nation's economy and national security.
- There is also a National Artificial Intelligence Research and Development Strategic Plan, produced in collaboration between OSTP and a number of other cross-government committees and working groups. This has been issued three times, in 2016, in 2019, and most recently in 2023.
- Additionally, relevant agencies have released numerous strategies and plans.

These strategies build on work by previous administrations, including a 2016 report from NSF on Preparing for the Future of Artificial Intelligence, and White House reports, including the 2022 Blueprint for an AI Bill of Rights that outlines protections that should be pursued as the use of AI accelerates.

It should be noted, however, that the U.S. Supreme Court issued a landmark decision on June 28, 2024 in *Loper Bright Enterprises v. Raimondo* that may greatly curtail the ability of federal government agencies to promulgate strategy and regulation relating to AI (and all other matters handled by federal agencies). The ruling may be expected to have an outsized impact on emerging and rapidly evolving technologies like AI because Congress has passed little legislation relating to AI, and agencies have been quicker to move on the many developing issues. It remains to be seen how Congress and agencies will respond to this development.

3. Has your country implemented rules or guidelines (including voluntary standards and ethical principles) on artificial intelligence? If so, please provide a brief overview of said rules or guidelines. If no rules on artificial intelligence are in force in your jurisdiction, please (i) provide a short overview of the existing laws that potentially could be applied to artificial intelligence and the use of artificial intelligence, (ii) briefly outline the main difficulties in interpreting such existing laws to suit the

peculiarities of artificial intelligence, and (iii) summarize any draft laws, or legislative initiatives, on artificial intelligence.

The U.S. has in place a range of guidelines and principles on artificial intelligence, the most significant of which is the 2023 Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. The executive order directs federal agencies to develop new standards for AI safety and security, protect privacy, address equity and civil rights concerns, and promote innovation while maintaining American competitiveness; many of these new standards have been released as drafts. Among other actions, the executive order directs regulation requiring developers of powerful AI systems to share safety test results with the government, establishes standards for watermarking AI-generated content, and develops best practices for AI use in critical infrastructure and various other sectors.

Prior to this executive order, several federal agencies had already issued AI-related guidelines.

- NIST AI Risk Management Framework: The National Institute of Standards and Technology (NIST) released its AI Risk Management Framework in January 2023, providing voluntary guidance to organizations on managing risks associated with AI systems.
- White House Voluntary AI Security Commitments: Companies developing Frontier Models have entered into voluntary commitments to ensure the safe, secure, and trustworthy development of AI systems by focusing on ensuring the safety of AI systems, protecting against cybersecurity threats to AI, and developing watermarking systems to help detect AI-generated content.
- FDA's AI/ML-Based Software as a Medical Device: Released in January 2021, this plan outlines the FDA's approach to regulating adaptive AI and machine learning in medical devices as part of existing premarket submission processes. The approach emphasizes a "total product life cycle" regulatory approach, which includes clear expectations for quality systems and "good machine learning practices," and focuses on the importance of real-world performance monitoring.
- Federal Trade Commission Guidance: The FTC has published guidance on using AI and algorithms fairly, emphasizing transparency, explainability, and accountability.
- State Regulations: States such as Tennessee, Colorado, and Utah have implemented their own AI-related regulations, particularly in areas like privacy and automated decision making. It is likely that additional states will soon follow.

Additionally, many relevant U.S. laws were intended to be "technology neutral" and apply to processes and outcomes rather than to the methods to achieve them, and therefore apply whether or not AI is used. Some examples include:

- *Financial:* The Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act, the Equal Credit Opportunity Act, the Dodd-Frank Wall Street Reform Act, and the Consumer Protection Act all provide a lens through which to examine well-established rules for eligibility decision making, credit reporting, and eligibility explainability.
- *Health:* The Department of Health and Human Services regulates discriminatory outcomes under a number of laws, including the Civil Rights Act, the Rehabilitation Act, the Age Discrimination Act, and the Affordable Care Act.
- *Insurance:* While many eligibility laws are federal, insurance is regulated by states; however, anti-discrimination rules at the federal level came into force with the Civil Rights Act.
- *Housing:* The Civil Rights Act and the Fair Housing Act both address discriminatory housing practices, including the use of background screening.
- *Employment:* The Equal Employment Opportunity Commission has rules around employment and hiring policies and practices that prohibit discrimination throughout the hiring and employment life cycle. These rules are increasingly applied throughout automated hiring and employment processes.

As noted in response to Question No. 2, the U.S. Supreme Court issued a landmark decision on June 28, 2024 in *Loper Bright Enterprises v. Raimondo* that may greatly curtail the ability of federal government agencies to promulgate strategy and regulation relating to AI. It remains to be seen how Congress and agencies will respond to this development.

4. Which rules apply to defective artificial intelligence systems, i.e. artificial intelligence systems that do not provide the safety that the public at large is entitled to expect?

Defective artificial intelligence (AI) systems in the United States may be subject to various legal rules and regulations that are intended to ensure safety, consumer protection, and liability for damages. The legal framework for defective AI systems is evolving, but it currently involves aspects of product liability, negligence, and consumer protection laws (in addition to the laws, regulations, and guidelines identified in response to Question No. 3 above).

a. Product Liability

Product liability laws hold manufacturers, distributors, and sellers accountable for placing defective products into the hands of consumers. AI systems, as products, may be subject to these laws. There are three main types of product defects:

- Design Defects: If the AI system's design is inherently unsafe.
- Manufacturing Defects: If the AI system deviates from its intended design during production.
- Marketing Defects: If there are inadequate instructions or warnings regarding the AI system's use.

Under product liability law, if strict liability applies, a plaintiff does not need to prove negligence, only that the product was defective and caused harm.

b. Negligence

A cause of action based on negligence may be available if it can be demonstrated that the developer or provider of an AI system failed to exercise reasonable care in the design, development, testing, or deployment of the system. A plaintiff would need to establish these elements:

- Duty of Care: The AI developer owes a duty to the user and the public to create a safe product.
- Breach of Duty: The developer failed to meet the standard of care.
- Causation: The breach of duty caused harm.
- Damages: There are measurable damages as a result.

c. Consumer Protection Laws

Consumer protection laws, such as those enforced by the Federal Trade Commission (FTC), can apply to AI systems. The FTC Act prohibits unfair or deceptive acts or practices. If an AI system fails to perform as advertised or poses safety risks, the FTC may take action against a company making or offering the system.

d. Federal and State Regulations

Several federal and state agencies have regulations that can apply to AI systems. These include:

Federal Trade Commission: Monitors and enforces consumer protection and privacy standards.

Food and Drug Administration: Regulates AI systems used in healthcare and medical devices.

National Highway Traffic Safety Administration: Regulates AI in automotive technologies, including autonomous vehicles.

State Laws: Various states have their own consumer protection laws and may have specific regulations pertaining to AI.

As noted in response to Question No. 2, the U.S. Supreme Court issued a landmark decision on June 28, 2024 in *Loper Bright Enterprises v. Raimondo* that may greatly curtail the ability of federal government agencies to promulgate strategy and regulation relating to AI. It remains to be seen how Congress and agencies will respond to this development.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems.

The civil and criminal liability that may follow in case of damages caused by AI systems tracks the underlying substantive laws that give rise to the liability. This is to say, a person or company that commits a crime or tort (or breach of contract) by means of an AI system will face the same liability as if the person or company had performed the culpable conduct without the use of an AI system. The use of an AI system in no way excuses or avoids liability and, at present, does not enhance or expand liability.

6. Who is responsible for any harm caused by an AI system? And how is the liability allocated between the developer, the user and the victim?

It is unclear as of July 2024 how liability will be allocated

between and among various parties. Although numerous class actions have been filed against companies building large language models and AI-related products (as detailed in responses below), few, if any, have progressed to a point where courts have provided substantive guidance on the allocation of liability for harm caused by an AI system.

7. What burden of proof will have to be satisfied for the victim of the damage to obtain compensation?

There is no indication yet that the burden of proof in cases arising from or related to the use of AI systems will be different from the burden of proof in other cases brought under the same substantive laws. Criminal prosecutions will always require proof of guilt beyond a reasonable doubt. Civil liability will usually follow where a preponderance of the evidence (i.e., proof that a thing is more likely than not) indicates the defendant performed or was responsible for the actions giving rise to liability. There are some frameworks in U.S. jurisprudence where liability may be premised upon "strict liability," where liability follows from the mere fact of performing the act that caused the harm (even in the absence of fault or criminal intent). There are no statutes or cases yet that have applied strict liability in relation to the use of AI systems. Even in the absence of new statutes that impose strict liability in relation to AI systems, it is foreseeable that courts may apply strict liability to AI-related cases where that is the standard applied by the underlying substantive law (e.g., certain construction and products liability cases).

8. Is the use of artificial intelligence insured and/or insurable in your jurisdiction?

The answer to this question is still unfolding. It is too early to tell whether insurers will cover the range of risks posed by AI. Insurers may cover some AI-related risks in existing insurance policies; alternatively, they may add endorsements or exclusions that expressly address AI-related risks. Currently, many insurers are asking more questions about prospective policyholders' use of AI during the underwriting process.

a. Cyber Liability Insurance

So-called cyber liability insurance policies generally provide coverage for first-party losses and third-party liabilities arising out of cyber incidents like network security events, data breaches, and ransomware attacks, but some cyber liability policies also provide coverage for less-common exposures that have heightened importance with the rise of AI, such as regulatory liability and media liability. In contrast, cyber liability policies generally do not provide coverage for breach of contract claims.

b. Technology Errors and Omissions Insurance

Technology errors and omissions (TE&O) insurance policies provide coverage for third-party claims that allege a wrongful act, error, or omission in the performance of technology services or the failure of a technology product to perform as intended. Unlike cyber liability policies, TE&O policies generally provide coverage for breach of contract claims. TE&O policies, however, typically exclude coverage for liability arising out of bodily injury or property damage. Thus, a key issue for companies providing AI-powered products or services that expose them to bodily injury or property damage liability will be whether their general liability insurance policies provide coverage for bodily injury or property damage claims arising out of AI-powered products or services.

c. General Liability Insurance

Commercial general liability (CGL) insurance policies generally provide coverage for third-party claims that allege bodily injury or property damage. CGL policies, however, often exclude coverage for professional liability claims. Furthermore, as an example, there is a standard professional liability exclusion that excludes coverage for third-party claims that allege bodily injury or property damage arising out of the selling, licensing, or furnishing of computer software. As a result, there may be a potential gap in coverage for companies that sell AI-powered software products or services that lead to bodily injury or property damage claims.

9. Can artificial intelligence be named an inventor in a patent application filed in your jurisdiction?

No, not at present. Both the U.S. Patent and Trademark Office (USPTO) and courts that have considered the issue have agreed that an inventor must be a "natural person," which excludes AI systems from being identified as inventors. However, while AI systems cannot be identified as inventors, USPTO guidance indicates that use of such systems by natural persons does not preclude the possibility of those natural persons obtaining a patent so long as the natural persons have contributed inventive subject matter to the invention. Litigation is still under way regarding this issue.

10. Do images generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to?

No, not at present. Both the U.S. Copyright Office and courts that have considered the issue have agreed that an author must be a "natural person," which excludes AI systems from being identified as authors. However, while AI systems cannot be identified as authors, the Copyright Office issued guidance in March 2023 indicating that use of such systems by natural persons does not preclude the possibility of those natural persons securing copyright protection so long as the natural persons have contributed original subject matter to the work. Litigation is still under way regarding this issue.

11. What are the main issues to consider when using artificial intelligence systems in the workplace?

There are many issues to consider when integrating AI systems into the workplace. While these issues span a range of areas, the following are some key ethical and legal considerations.

Bias and Fairness: AI systems can perpetuate and amplify biases present in training data, leading to unfair treatment of employees or applicants. It is crucial to ensure that AI algorithms are developed and trained on diverse and representative data sets.

Transparency and Explainability: Employees and stakeholders should understand how AI systems make decisions, especially in critical areas like hiring, performance evaluations, and promotions. AI systems should be explainable and transparent.

Privacy: The use of AI systems often involves collecting and processing large amounts of data. It is essential to respect and protect employee privacy, ensuring compliance with data protection laws and regulations.

Employment Laws: AI systems must comply with existing employment laws and regulations, such as non-discrimination laws and labor standards.

Data Protection Laws: AI systems must comply with data protection laws like the General Data Protection Regulation in the EU or the California Consumer Privacy Act in the U.S. These laws govern how personal data is collected, processed, and stored.

Intellectual Property: Companies must consider the infringement exposure that may follow, both in relation to the technical operation of an AI system and in relation to a system's output. Companies ought also to consider the protectability of their own inventions and works.

12. What privacy issues arise from the use of artificial intelligence?

AI operates on data, often at all points in its development life cycle. Thus, the use of AI can raise questions about the appropriate use of data and unauthorized disclosures of personal information based on the data these systems may collect, process, and analyze. This may include biometric data, financial records, health information, and behavioral patterns.

AI systems often centralize large volumes of personal data and may become attractive targets for cybercriminals. The complexity of AI algorithms can also make it challenging to detect and prevent data leaks or misuse. Additionally, the use of AI in decision-making processes, particularly in areas like employment, credit scoring, or law enforcement, raises concerns about transparency and the right to privacy in decision making. Individuals may not be aware of how their personal data is being used to make decisions that affect them, or have the ability to challenge these decisions effectively. This lack of transparency and control over personal information processed by AI systems poses significant challenges to established privacy principles and legal frameworks.

13. How is data scraping regulated in your jurisdiction from an IP, privacy and competition point of view?

There is no unified framework for regulation of data scraping in the U.S. The U.S. does not have sui generis data protection, as exists, for example, in the EU. However, several types of laws may apply. These include copyright, contract, and misappropriation law.

Copyright. There is neither per se liability for copyright infringement nor a blanket "fair use" exception to copyright liability for copying and/or making derivative works of copyrightable works that are collected by means of data scraping. Operators of large language models are arguing in pending litigation in the U.S. that data scraping to train their models is a form of fair use. It will be some years before the courts reach a final determination of this issue under current copyright law, and it is possible the U.S. Congress will amend copyright law in the meantime or after such a final court determination. It bears

mentioning that copyright law in the U.S. protects the expression of ideas, not ideas themselves or unarranged data. So, a threshold determination in a copyright claim brought in relation to data scraping is whether the scraped data is protectable under copyright in the first instance.

Contract. Information made available pursuant to a contract is governed by the terms of the contract, and parties to a contract may agree that certain copying is not permitted even if copyright law would otherwise allow it. There have been cases in the U.S. that found liability for data scraping on the basis of a trespass theory (specifically "trespass to chattels"). These cases generally have been premised on a website proprietor alerting visitors that scraping was prohibited and that prohibition (coupled with proof of harm) made the scraping a trespass.

Misappropriation. Some states in the U.S. have found liability for misappropriation of information, but this doctrine is quite limited because federal copyright law preempts inconsistent state laws. Put another way, the federal framework that authorizes or declines to authorize the "owner" or publisher of certain information to bring a copyright infringement claim is exclusive, and unless liability under state law includes an added element (beyond mere copying), the state law will not be permitted to prohibit what is authorized by federal copyright law.

Computer Fraud and Abuse Act. Some website proprietors have argued over the years that data scraping is a violation of the 1986 federal Computer Fraud and Abuse Act, which provides for both criminal and civil liability, depending on the conduct and circumstances. In the present context, the Act generally prohibits actions that damage protected computers, that involve taking of certain financial information, and that involve committing fraud using a computer. Additional protections are available for government computers. Recent case law has significantly limited the applicability of the Act in cases of data scraping of private commercial websites on the open internet. It is currently unclear whether a cause of action under the Act remains for this conduct.

Privacy. Information that is subject to scraping on the open internet is not likely to be protectable under general privacy regimes because the information is not private.

Competition. Competition law (or antitrust law in the U.S.) does not have any particular applicability to data scraping. Acts that give rise to liability under antitrust law will do so regardless of the technical means involved to perform the acts.

14. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

The enforceability of website terms of use in the U.S. tracks general principles of contract law. A binding contract may be formed where terms are offered by one party and accepted by another party. The challenge in terms-of-use cases is that website visitors may be unaware of proposed contract terms and may not have accepted them, including whatever restrictions may be included in regard to data scraping. This challenge may be overcome by presenting contractual terms in a more prominent manner. For example, requiring a party to scroll through contractual terms and select an "I agree" checkbox will more likely result in an enforceable contact than terms of use under a link to "Legal Terms" in small text at the bottom of a webpage. A prohibition on data scraping in an otherwise enforceable contract will be enforceable; it is not the case that such a prohibition would be prohibited by current law as, for example, contrary to public policy. Some websites use the Robots Exclusion Protocol by including the robots.txt filename on their sites. This is an electronic signal to web crawlers that they are not authorized to scrape a site. Compliance with the protocol is voluntary, and there is no enforcement mechanism. However, the operator of a web crawler that ignores this instruction may be on notice that data scraping is not authorized, and this may help support other legal claims, such as trespass to chattels (discussed above).

15. Have the privacy authorities of your jurisdiction issued guidelines on artificial intelligence?

Several U.S. agencies with jurisdiction over privacy have issued guidelines on artificial intelligence, reflecting this recognition of AI's impact on data protection and privacy.

- The Federal Trade Commission: The FTC has been particularly active in this area. In April 2020, the FTC released guidance on using AI and algorithms, emphasizing the need for transparency, explainability, fairness, accuracy, and accountability. The guidance warns against exacerbating bias or unfairness and highlights the importance of robust data security measures. More recently, FTC leadership has made it clear that it intends to scrutinize the use of AI, companies developing advanced AI systems, and companies making AI investments and partnerships.

- The National Institute of Standards and Technology: NIST has developed a risk management framework for AI systems, which includes privacy considerations and is consistent with the NIST Privacy Framework.
- White House: Many White House actions, including the 2022 Blueprint for an AI Bill of Rights and the AI Executive Order (discussed above), include principles on data privacy and algorithmic discrimination.
- States: The California Privacy Protection Agency is developing regulations that will include provisions on automated decision making and profiling using AI. Similarly, the Colorado Attorney General's Office has issued draft rules under the Colorado Privacy Act that address AI-driven profiling. Other states, such as New York and Washington, have task forces or working groups examining the implications of AI, including privacy concerns.

As noted in response to Question No. 2, the U.S. Supreme Court issued a landmark decision on June 28, 2024 in *Loper Bright Enterprises v. Raimondo* that may greatly curtail the ability of federal government agencies to promulgate strategy and regulation relating to AI. It remains to be seen how Congress and agencies will respond to this development.

16. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence?

The Federal Trade Commission has been active in addressing cases involving artificial intelligence. In 2023, the FTC brought a case against Rite Aid alleging that its use of AI facial recognition technologies did not include reasonable safeguards and falsely tagged people, primarily women and people of color, as shoplifters. In 2021, the FTC brought a case against Everalbum alleging unlawful use of facial recognition technology and deceptive practices regarding users' ability to opt out of this AI-driven feature. This case resulted in a settlement requiring the company to delete models and algorithms developed using improperly obtained biometric data. The FTC has also investigated and settled cases involving AI-powered credit scoring systems, such as a 2020 case against Ascension Data & Analytics for failing to ensure the security of personal information used in its AI models.

As noted in response to Question No. 2, the U.S. Supreme Court issued a landmark decision on June 28, 2024 in *Loper Bright Enterprises v. Raimondo* that may greatly curtail the ability of federal government agencies to promulgate strategy and regulation relating to AI. It remains to be seen how Congress and agencies will respond to this development.

17. Have your national courts already managed cases involving artificial intelligence?

There are many cases pending on a variety of issues. Some have reached initial decisions, but the law is still developing in this area. In addition, following some widely reported examples of parties filing error-riddled briefs prepared by generative AI systems, several courts and judges have issued standing orders that require parties to disclose when they have used generative AI in preparing court filings. The following are some examples of pending cases involving AI, though there are many more examples. Several of these cases are putative class actions, though no classes have yet been certified.

Patent

- *Thaler v. Vidal,* 43 F.4th 1207, 1213 (Fed. Cir. 2022), *denied*, 143 S. Ct. 1783 (2023): USPTO took the position that inventors must be natural persons, and the Federal Circuit affirmed. The Supreme Court declined to review the case, possibly to allow the law in this space to develop further before weighing in.

Copyright

- *UMG Recordings, Inc. v. Suno, Inc.*, No. 1:24-cv-11611 (D. Mass., filed June 24, 2024): Multiple record companies coordinated by the Recording Industry Association of America allege that Defendants have infringed their sound recording copyrights by creating an AI platform that produces digital music files that sound like well-known musical artists.
- *Nazemian v. Nvidia Corp*., No. 3:24-cv-1454 (N.D. Cal., filed Mar. 8, 2024): A group of authors brought a copyright infringement suit against Nvidia, alleging that Nvidia copied and used their copyright-protected works to train its NeMo Megatron series of LLMs.
- *O'Nan v. Databricks Inc.*, No. 3:24-cv-01451 (N.D. Cal., filed Mar. 8, 2024): A group of authors brought a copyright infringement suit against MosaicML for direct infringement and Databricks, Inc. for vicarious infringement concerning the training of Mosaic's MPT LLM model series, including MPT-7B and MPT-30B.
- *Raw Story Media, Inc. v. OpenAI, Inc.*, 1:24-cv-01514 (S.D.N.Y., filed Feb. 28, 2024); *The Intercept Media, Inc. v. OpenAI, Inc.*, No. 1:24-CV-01515 (S.D.N.Y., filed Feb. 28, 2024): Two suits were filed by news media organizations against OpenAI, alleging that OpenAI violated the Digital Millennium Copyright Act by

training the ChatGPT LLM with copies of their works from which content management information had been removed.
- *Basbanes v. Microsoft Corp.*, No. 1:24-cv-00084 (S.D.N.Y., filed Jan. 5, 2024): A class action complaint was filed by journalists and authors of nonfiction works against Microsoft and OpenAI alleging that the companies unlawfully reproduced their copyrighted works for the purpose of training their LLMs and ChatGPT. This case has been consolidated with *Authors Guild v. Open AI Inc.*, No. 1:23-cv-08292 (S.D.N.Y., filed Sept. 19, 2023), and *Alter v. Open AI Inc.*, No. 1:23-cv-10211 (S.D.N.Y., filed Nov. 21, 2023).
- *New York Times v. Microsoft Corp.*, No. 1:23-cv-11195 (S.D.N.Y., filed Dec. 27, 2023): Alleges Microsoft and OpenAI extensively copied *New York Times* reporting to train Defendants' large language models.
- *L. v. Alphabet Inc.*, No. 3:23-cv-03440 (N.D. Cal., filed July 11, 2023): Alleges Google stole content created by "hundreds of millions of Americans" to develop its AI chatbot Bard and other AI systems, giving Google an unfair advantage over competitors that obtain data legally for AI training.
- *Silverman v. OpenAI, Inc.*, No. 3:23-cv-03416 (N.D. Cal., filed July 7, 2023): Alleges OpenAI used copyrighted books as training material for the large language models that power ChatGPT.
- *Kadery v. Meta Platforms, Inc.*, No. 3:23-cv-03417 (N.D. Cal., filed July 7, 2023): Accuses Facebook of exploiting copyrighted books as training material for its LLaMA program.
- *Tremblay v. OpenAI, Inc.*, No. 3:23-cv-03223 (N.D. Cal., filed June 28, 2023): Alleges that copyrighted material from Plaintiffs' published books was improperly ingested and used to train ChatGPT.
- *Getty Images (US), Inc. v. Stability AI, Inc.*, No. 1:23-cv-0135 (D. Del., filed February 3, 2023): Alleges that the Stability AI's image generator, Stable Diffusion, infringed Getty's copyrights in over 12 million photographs copied from Getty's website, removed or altered copyright management information (CMI), provided false CMI, and infringed its trademarks, all despite terms of use on Getty's website expressly prohibiting such uses.
- *Andersen v. Stability AI Ltd.*, No. 3:23-cv-00201 (N.D. Cal., filed Jan. 13, 2023): Plaintiff artists allege their works were used without permission as input materials to train and develop various AI image generators that create works in the style of the artists, which the artists argue are unauthorized derivative works. Plaintiffs also claim Defendants are liable for vicarious copyright infringement and for altering or removing CMI from the images owned by Plaintiffs. Defendants include Stability AI, Inc., Midjourney, Inc., and DeviantArt, Inc.
- *Doe v. GitHub, Inc.*, No. 3:22-cv-06823 (N.D. Cal., filed Nov. 3, 2022): Alleges a violation of 17 U.S.C. 1202 (circumvention of copyright protection systems protecting software against unauthorized copying) in connection with unauthorized use of Plaintiff programmers' software code to develop Defendants' AI machines, Codex and Copilot. Defendants include GitHub, Inc., Microsoft Corp., and OpenAI, Inc.

Privacy

- *L. v. Alphabet Inc.*, No. 3:23-cv-03440 (N.D. Cal., filed July 11, 2023): Cited above regarding copyright claims, this action also brings privacy-related claims.
- *M. v. OpenAI LP*, No. 3:23-cv-03199 (N.D. Cal., filed June 28, 2023): Claims the improper collection, storage, tracking, and sharing of individuals' private information through web scraping without consent misappropriates personal data on an "unprecedented scale."

Tort

- *Walters v. OpenAI,*LLC, No. 23-A-04860-2 (Ga. Super. Ct. Gwinnett Cty., filed June 5, 2023): Alleges OpenAI defamed Plaintiff by fabricating story that Plaintiff was involved in certain litigation.

Discrimination

- *Mobley v. Workday, Inc.*, No. 3:23-cv-0070 (N.D. Cal., filed Feb. 21, 2023): Claims that AI systems used by Workday, which rely on algorithms and inputs created by humans, disproportionately impact and disqualify Black, disabled, and older job applicants.
- *Huskey v. State Farm Fire & Casualty Co.*, No. 1:22-cv-07014 (N.D. Ill., filed Dec. 14, 2022): Claims State Farm's algorithms and tools display bias in the way they analyze data.

18. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence?

The U.S. does not have a single, dedicated regulator responsible for overseeing the use and development of artificial intelligence across all sectors. For now, the U.S. approach to AI governance remains largely sector-specific and decentralized, with various agencies adapting existing regulatory frameworks and pursuing new rules. For instance, the Federal Trade Commission has taken a leading role in addressing AI-related consumer protection and competition issues. The Equal

Employment Opportunity Commission has begun to tackle AI's impact on workplace discrimination. The Food and Drug Administration is developing frameworks for AI in medical devices, while the National Highway Traffic Safety Administration is addressing AI in autonomous vehicles. Additionally, the National Institute of Standards and Technology has been tasked with developing an AI Risk Management Framework, which, while not regulatory, provides guidance for the responsible development of AI systems. Efforts among these agencies have been coordinated by the White House Office of Science and Technology Policy's National AI Initiative Office, which does not have regulatory authority.

19. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited?

The use of artificial intelligence by businesses in the U.S. is widespread and growing rapidly. Many business software platforms, including email, word processing, and research services, have incorporated AI-enhanced functions into their products. Some of these functions include drafting short messages and editing/correcting text. It bears mentioning that the extent of use varies greatly, depending on the type of AI under consideration and the industry. Use of generative AI to create images, software, and completed documents may not be widespread yet, but use of autocorrect and voice-operated systems like Siri and Alexa, to the extent these are considered forms of AI, is pervasive.

20. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how?

Lawyers in firms and at companies are in the early stages of exploring and making use of AI technologies in their practices. Many legal research and document/information management providers are integrating AI functions into their offerings. Many of these platforms have been cautiously trained on licensed or public domain information. After some well-publicized incidents of lawyers filing error-filed court papers created by ChatGPT, some lawyers are leery of adopting AI in their practices. Lawyers are also concerned about protection of confidentiality and attorney-client privilege and, as a result, may be slower to adopt these technologies than some other industries. That being said, even a casual observer of the legal field can see that AI tools will eventually transform the legal industry and impact the way attorneys work, how law firms are managed, and how legal decisions are made.

Here are some illustrative examples of how AI is being used in the legal sector:

- Due Diligence and Document Review: AI can quickly review vast amounts of data and documents, identify key points, and draw attention to relevant provisions. AI tools can process contracts and flag clauses responsive to diligence requests or disclosure requirements. This significantly reduces the time and effort needed for legal professionals to review documents.
- Legal Research and Predictive Analysis: Related to document review, AI can sift through many cases, regulations, and rules to identify relevant precedent and clauses. AI can also analyze prior decisions and judgments to predict possible outcomes of ongoing disputes to assist in devising legal strategy.
- Contract Generation: AI tools can be used to automate the creation of legal agreements based on set parameters or letters of intent, and they can flag non-standard clauses, check compliance with legal requirements, or highlight critical agreements that are due for renewal or require re-negotiation.
- Chatbots and Ideation: AI-powered chatbots can provide legal direction on simple matters, reducing the time lawyers need to spend on routine queries or producing general client communications.
- Administrative Matters: AI can automate administrative tasks such as billing and time-tracking, reducing errors and freeing up more time for legal professionals to produce higher-level, complex legal work.

Law firms and attorneys can be expected to adopt AI tools from commercial providers that are fine-tuned specifically for legal work. Even with the availability of "safer" AI tools, law firms and attorneys will still need to consider frameworks for ethical and responsible use of AI, training of individual attorneys, and careful review of outputs for relevancy, accuracy, truthfulness, and completeness.

21. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Challenges

1. Learning about and training on the many types of specialized AI systems that are available and being used by clients and other lawyers. This implicates legal ethics and even

malpractice issues relating to competence, confidentiality, and other duties.
2. Understanding the operational details of AI systems, including the corpus of original/training data used in an AI system, how the training data is processed and used, whether prompts/queries are used for further training, and whether and how confidentiality is preserved.
3. Tracking the many laws promulgated by legislators and courts and case law at the federal and state level (not to mention internationally) that are relevant to advising clients and to guiding lawyers' own practices.
4. Avoiding unintentional bias and lack of transparency by use of AI systems that may lead to unfair or discriminatory outcomes.
5. Balancing cost and time with risk and benefit while keeping pace with peers and properly serving clients.

Opportunities

1. There is great client demand for counseling, negotiation, and in some cases litigation related to AI issues, and this can be expected to continue for some years.
2. AI tools will provide a wide variety of efficiencies in lawyers' own practices, including review and drafting of documents, analysis of large collections of documents (e.g., in discovery in litigation), and evaluation of potential case outcomes. These efficiencies should enable lawyers to spend more time on strategic thinking and to handle a greater number of matters.
3. AI tools may raise both the floor and the ceiling in terms of the quality of legal services lawyers are able to provide.
4. AI tools may reduce the cost of some types of legal services, making legal counsel available to people who could not previously afford it.
5. AI tools may help drive lawyer satisfaction, as certain routine tasks are automated and more time is available for "higher-level" tasks.

22. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months?

The most significant legal developments in the next 12 months are likely to come in the form of legal regulation, whether by executive orders, agency action, or legislation. Litigation is slow-moving, and the principles established in pending cases will not gel until appeals are exhausted, different states and circuits have their say, and (potentially) the Supreme Court weighs in on major issues. It can be expected that these developments will address a wide range of topics, including intellectual property law, privacy, consumer protection, public safety, antidiscrimination, and employment practices.

Contributors

Justin Pierce
Partner
jepierce@venable.com

Eric Prager
Partner
eaprager@venable.com

Ryan Ward
Counsel
rtward@venable.com

Heather West
Senior Director of Cybersecurity and Privacy Services
hewest@venable.com