



**ArentFox
Schiff**

ArentFox Schiff
Industry Guide to
Artificial Intelligence

Fall 2023



**Smart In
Your World**

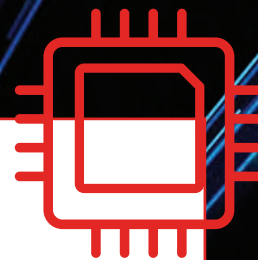
afslaw.com

“There is nothing that will happen in our lifetime that is more existential than AI, and business leaders are grasping with what to do about it. Companies that lean into it will survive, and those that don't, won't survive.”

Anthony V. Lupo
Chairman

Industries Covered

Automotive AI	5
Consumer Products AI	11
Energy & Cleantech AI	15
Fashion & Retail AI	18
Government Relations AI	23
Health Care AI	28
Hospitality AI	32
Life Sciences AI	37
Long Term Care & Senior Living AI	40
Nonprofits & Associations AI	44
Privacy, Data Protection & Data Security AI	48
Private Companies AI	53
Sports AI	56



A Message From Our Chair

Embracing **Artificial Intelligence** for Future Industry Success

As chairman of a forward-thinking enterprise that was among the first law firms to have a presence on the Internet, operating at the cutting edge of AI, web3, Metaverse, and blockchain innovation is in our DNA.

Recent advancements make it clear that AI is moving at breakneck speed and is sure to transform industries, streamline processes, and drive growth. Companies that fail to adapt to these changes risk being left behind. In short, nothing in our lifetime presents more of an existential test than AI — and that's why ArentFox Schiff is providing clients with a 360-degree view of the opportunities and challenges in your rapidly evolving industry.

AI holds great promise to revolutionize the way we work, providing tools to make smart decisions and optimize efficiency. From automating routine tasks to enhancing customer experiences, technological advancements are poised to redefine business operations, supply chains, and workplace culture. Understanding how to leverage AI and navigating the hurdles specific to your industry will be essential to remaining competitive.

I would encourage industry leaders to embrace AI — not fear it — as the future success of all businesses and the global economy depend on it. Our law firm, which has already embarked on the journey to harness the power of AI, put together this guide to help you get started. We stand ready to partner with you to shape the business landscape for generations to come.

Anthony V. Lupo
Chairman



Our Comprehensive Legal **AI** Services

ArentFox Schiff is a top legal advisor in emerging technologies for global fashion brands, sports teams, athletes, media companies, and creators. Our AI, Metaverse & Blockchain Industry Group helps clients understand the regulatory landscape surrounding AI, ensuring compliance with relevant laws and regulations. With our knowledgeable guidance, businesses can confidently leverage the power of AI and navigate the ever-changing legal landscape with ease.

How We Support Businesses

We offer comprehensive AI legal services to ensure businesses stay compliant, protected, and prepared for the future.

Regulatory Compliance: Assist with adherence to data privacy and security laws, including GDPR, CCPA, and CPRA

Contracts & Agreements: Draft and negotiate AI-related contracts, such as licensing, data sharing, and service level agreements

Intellectual Property Rights: Advise on fair use, authorship, ownership, copyrightability, and secure patents and trademarks for AI innovations

Due Diligence: Perform thorough assessments on AI-related transactions to identify potential legal risks and liabilities

Litigation: Represent clients in AI-related disputes, including IP rights, data breaches, and bias

Ethics & Transparency: Guide clients on ethical considerations of AI and promote responsible technology use and algorithmic transparency

Risk Management: Develop strategies to manage potential legal risks involved in AI integration into businesses

Mergers & Acquisitions: Ensure seamless transitions and full legal compliance during AI-focused M&A

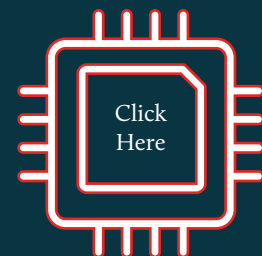
Innovation & Development: Provide strategic legal advice for AI-driven business innovations

Employment & Workplace: Navigate legal complexities of AI in the workplace, including labor laws, privacy concerns, and employee training programs

Ready to Use GenAI? Understand Your Rights With Our “Terms of Use” Cheat Sheet

Generative AI tools vary in how they can be used and how they protect your information. The best way to manage your risk and protect your privacy is by reviewing each tool’s Terms of Use. We are monitoring key terms of use provisions for the most popular GenAI tools.

Get a sample of the **AFS GenAI Terms of Use Cheat Sheet**





Self-Driving

Automotive AI

48
mph

100m

AUTOMOTIVE

On the Road With Generative AI: Key Legal Considerations for the Automotive Industry

[Aaron Jacoby](#), [Veronique H. Tu](#), [D. Reed Freeman](#), [Robert D. Boley](#)

Generative AI is already an integral part of the automotive industry, playing a significant role in enhancing Advanced Driver Assistance Systems (ADAS) and making it possible for drivers to interact with their vehicles. Generative AI produces and processes massive amounts of data and images to train and improve self-driving algorithms. AI provides drivers with enhanced in-vehicle connectivity using voice technology, real-time traffic, and automatic rerouting, and the ability to monitor vehicles and advise if there's a mechanical problem developing or that it's time for service. Looking toward the future, manufacturers are using ADAS technologies and generative AI as building blocks to develop fully autonomous vehicles that one day can cruise across the country without any input from humans.

ADAS and Autonomous Driving

Many people use the terms "ADAS" and "autonomous driving" interchangeably, but they are not actually the same thing. [ADAS](#) is the suite of automotive technologies that assists drivers with features such as collision avoidance, pedestrian detection/avoidance, blind spot detection, lane keeping assist, adaptive cruise control, traffic sign recognition, and parking assistance. Sensors and advanced processing from camera, radar, sonar, thermal imaging, infrared sensors, and lidar systems help provide accurate event detection, driver alerts, and semi-autonomous intervention for ADAS.

The term "autonomous driving" refers to the technology that allows cars to drive without any human intervention. There are six levels of autonomous driving (named [Levels 0 to 5](#)) each with its own set of requirements and capabilities. Today's vehicles that have a suite of ADAS technologies are Level 2+ and Level 3. At Level 2 vehicles can operate autonomously with complex functions such as steering, braking, and accelerating but the driver should still be aware and in control. Level 2 automation includes [Ford BlueCruise](#), [Tesla Autopilot](#), and [GM Super Cruise™](#). Level 3 vehicles have conditional automated driving functions that allow a driver to disengage from driving while still sitting behind the wheel but must be prepared to take over in certain situations. At Level 3 a vehicle can monitor its surroundings, change lanes, control steering and braking, and even accelerate past a slow-moving vehicle.

Level 4 automation will reduce a driver's involvement to the point where it will be possible to work on a laptop or watch a movie. Test vehicles from [Cruise](#), a subsidiary of General Motors, and [Waymo](#), a spinoff from Google, are examples of Level 4 autonomy. Both Cruise and Waymo operate driverless ride-hailing services (with and without safety drivers) in Phoenix, San Francisco, Los Angeles (Waymo), and Austin (Cruise). Both companies are seeking approval from the California Public Utilities Commission to charge fares for their robo-taxi services in San Francisco that will have no one sitting in the driver's seat.

The highest level of autonomous driving is Level 5. A few automotive companies are testing Level 5 but a fully autonomous vehicle is not yet available to the public. This level represents a vehicle that can operate completely autonomously in all situations and does not require any human input.

ADAS technologies combine generative AI with vision, radar, and lidar sensor systems. Vision-based systems use image signal processing algorithms to identify and detect objects in their field of view. Onboard automotive cameras installed in the front, rear, and both the sides of the vehicle are the eyes of the vehicle and assist by sending collision warning alerts, providing vehicle parking assistance, performing object recognition, and offering lane change assistance and more. Radar is used when automotive cameras are insufficient in providing ADAS data in poor weather and low-visibility conditions. Radar-based systems have a longer range and they can also pass through objects and can detect the position and velocity of approaching vehicles and other objects on the road. Lidar (Light Detection Imaging and Ranging) sensor systems can see through objects and differentiate between on-road objects like vehicles, pedestrians, people, bikes, etc. Transmitters send out laser pulses that then bounce back off surfaces and return to the lidar sensor. The time it takes for each light pulse to return to the device informs it of the exact location of the surface the light hit. By creating and combining hundreds of thousands of data points per second, the lidar system can detect the shape of objects, follow moving obstacles, and create an accurate, real-time perception of the area. This provides a highly accurate object detection and recognition for safer and more efficient driving. Ford BlueCruise, which is a Level 2 ADAS, uses both an advanced camera and radar-sensing technologies to allow a driver to operate hands-free on pre-qualified sections of divided highways. A driver-facing camera in the instrument cluster monitors eye gaze and head position to help ensure the driver's eyes remain on the road. Ford uses AI to improve the system's capabilities through machine learning. Data is collected from owners who have opted in to share real world information from their vehicles. The algorithm learns by looking at video and different environmental and lighting conditions from sections of pre-qualified divided highways. The system also takes cues from drivers and their reactions to other vehicles on the highway such as moving over if there are larger vehicles next to them.

AI, Navigation, Infotainment Systems & Biometric Identifiers

Navigation and infotainment systems have become more intuitive and personalized with the use of generative AI. Companies like Waze use generative AI to provide real-time, personalized navigation suggestions based on user preference and traffic conditions. Machine learning algorithms can analyze a driver's music preferences and follow voice commands allowing for hands-free operation. The new 2023 [Genesis GV60](#) uses biometric identifiers with Face Connect and Fingerprint Authentication. Face Connect allows the vehicle to recognize the driver's face to lock or unlock its doors without a key. Once the user touches the door handle, a near-infrared (NIR) camera embedded into the vehicle's B-pillar analyzes unique facial features, such as the contours of the face and specific facial landmarks which the car can instantly identify as its owner during both daytime and even in the dark. The camera uses image recognition technology based on deep learning to detect registered faces. The feature allows owners to pre-register multiple profiles for families with multiple drivers. Once the system recognizes the driver it can create a cockpit environment according to previously saved personalize settings. The head-up-display, steering wheel, side mirrors, and infotainment settings are adjusted based on the driver's customized settings. The Fingerprint Authorization System allows the vehicle to be started without a key. This biometric authentication technology is similar to what everyone uses through their smartphones.

Key Legal Considerations for Auto Manufacturers and Suppliers

As legacy manufacturers and parts suppliers continue development and testing of autonomous vehicles with generative AI, there are several key issues to consider:

1. Cybersecurity

Autonomous vehicles are highly complex and connected devices that utilize a combination of high-tech sensors and innovative algorithms to detect and respond to surroundings. The vehicle is a blend of networked components, some existing within the vehicle, and others outside of it. These complex systems allow the vehicle to make complex decisions but it also allows hackers several avenues to exploit this emerging technology. In 2015, security researchers Charlie Miller and

Chris Valasek [remotely hacked a Jeep Cherokee](#) traveling at high speeds on the highway and forced it to come to stop in the middle of traffic. Using its internet connect, they were able to remotely gain control by exploiting vulnerabilities within Chrysler's Uconnect system. Similar vulnerabilities were found in Volkswagen, Tesla Model S, and BMW vehicles.

Companies must constantly develop procedures to protect their security architecture, intrusion detection, and anomaly detection. This includes encryption and authentication of the driver, and firewalls between a vehicle's internal network and the external world. Autonomous vehicles interact with a larger network of connected devices which include other vehicles, traffic signs, and even pedestrians with smart devices. Hackers could intentionally make a vehicle misinterpret a stop sign which would compromise both cybersecurity and the AI system to disrupt safety-critical functions.

2. Data Privacy

Generative AI often requires access to personal or sensitive information to authenticate authorized use. Sensor data is collected to help the vehicle understand where it is relative to other objects on the road. Data sets collected also include location data, i.e., destination, speed, and route data with additional information relevant to the trip. AI uses the data set associated with a particular vehicle to personalize and enhance navigation features including the option to save specific locations in order to plan personalized routes for drivers. If a hacker gains access to this data, information about the owner or passengers, such as where they live and work and the specific locations they frequent (which can be very sensitive information), could be compromised and misused. If this data is not properly protected, hackers can access a driver or passenger's personal information, leading to identity theft and misuse of personal information.

Manufacturers should [minimize](#) collection and retention of personal data to only what is needed for the AI system to function properly to reduce the risk of potential privacy breaches. Before using data for training generative AI, personal information should be deidentified to ensure individuals cannot be identified from generated outputs. Manufacturers using generative AI tools should clearly communicate to vehicle occupants their data collection, storage, and usage practices, and should only process personal data for disclosed purposes. Individuals should have granular control over what data they share and generate. If individuals wish to opt out of sharing their personal data through an AI system, it should be easy for them to manage their data. This is a very active area of the law at the federal and state levels, with [California's Privacy Protection Agency](#) leading the way as it considers new rules for AI and automated decision-making technology, which may trigger rights to access information about, and to opt out of business's use of these technologies, and obligations to perform risk assessments of their technologies.

3. Biometric Privacy

Technologies such as fingerprint readers, facial scanners, iris scans, and voice recognition collect and use biometric data to improve a driver's in-vehicle experience. Companies that collect this data must comply with privacy and data protection regulations to keep data private and secure. State privacy laws including the California Consumer Privacy Act ([CCPA](#)) require manufacturers and service providers to conduct data inventories and monitor the flow of data to be able to develop systems for compliance. The Illinois Biometric Information Privacy Act (BIPA) is one of the most stringent and [heavily litigated](#) biometric privacy laws in the country. BIPA regulates the collection, use, storage, retention, and destruction of biometric identifiers and biometric information. A "biometric identifier" is a biologically unique personal identifier, including a fingerprint, voiceprint, face geometry, or a retina or hand scan. "Biometric information" is any information based on an individual's biometric identifier used to identify an individual. BIPA imposes a number of compliance obligations on entities collecting biometric data, including providing notice, obtaining written consent, and developing a publicly available retention and destruction policy. Failure to comply with BIPA's requirements could subject companies to [substantial damages awards](#).

4. Regulatory Landscape

In 2021, the National Highway Traffic Safety Administration (NHTSA) issued a [Standing General Order](#) that required manufacturers and operators of automated driving systems (ADS) and SAE Level 2 ADAS-equipped vehicles to report

crashes to the agency. ADS is still in development, encompassing Level 3 and Level 5 vehicles. The Order allowed NHTSA to obtain timely and transparent notification of real-world crashes associated with ADS and Level 2 ADAS vehicles. In June 2022, NHTSA upgraded a preliminary investigation of Tesla’s Autopilot active driver assistance system to an [engineering analysis](#). As part of this evaluation, [NHTSA requested information](#) related to “object and event detection and response (OEDR) that include monitoring the driving environment (detecting, recognizing, and classifying objects and events, and preparing to respond as needed) and executing an appropriate response to such objects and events.”

In June 2023, NHTSA issued a [Second Amended Standing General Order](#). Not only is NHTSA reviewing driver behavior during real-world crashes, it is also examining the decisions by software algorithms that analyze data inputs in real time to determine the appropriate vehicle response as well as safety issues that may also arise from the operational design domain for the ADS, and the continuing evolution and modification of these systems through software updates (including over-the-air-update). NHTSA defines operation design domains as the operating conditions under which a given ADS or ADS feature is designed to function. This includes but is not limited to, environmental, geographical, and time-of-day restrictions, and/or the presence or absence of certain traffic or roadway characteristics.

On a national level, the federal regulatory framework has not been able to keep pace with the development of autonomous vehicles. States have filled this landscape creating a patchwork of regulations. NHTSA is in the process of formulating a framework to ensure automated driving systems are deployed safely.

5. Litigation

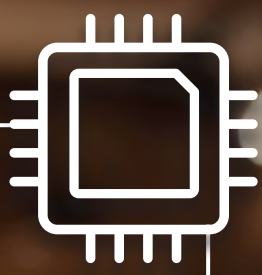
Who is at fault in an accident with a self-driving car? Is it the AI? Is it the human driver? In 2018 a self-driving Uber Volvo hit and killed a pedestrian named Elaine Herzberg who was jaywalking at the time. Her death was the first pedestrian fatality involving a self-driving car. The NTSB [concluded](#) that the vehicle could not determine if the woman was a pedestrian, a bicycle, or another car and could not predict where she was going. The safety driver, Rafaela Vasquez, was not looking at the road and was instead watching “The Voice” on her smartphone. The NTSB split the blame among Uber, the company’s autonomous vehicle, the safety driver in the vehicle, the victim, and the state of Arizona. Arizona prosecutors charged Ms. Vasquez with negligent homicide. Her trial originally scheduled for June 2023 has been delayed until at least September. Prosecutors found Uber not criminally liable for Ms. Herzberg’s death.

In a Columbia University [study](#), researchers developed a game-theory model that regulated the drivers, the self-driving car manufacturer, the car itself, and lawmakers. Lead author of the paper, [Dr. Xuan \(Sharon\) Di, said](#), “We found that human drivers may take advantage of this technology by driving carelessly and taking more risks, because they know that self-driving cars would be designed to drive more conservatively.” With more autonomous vehicles taking to the road in the future, there is a greater likelihood that liability will fall on manufacturers as there will no longer be a human safety driver to take over the vehicle if needed. Once a Level 5 vehicle is approved for use on the road without human intervention, who becomes liable for an accident – is it the manufacturer, the AI algorithm, or perhaps the engineer that wrote the algorithm?

6. Ethical Considerations

Autonomous vehicles are not “programmed” by humans to mimic human decision-making. Instead they learn from large data sets to perform tasks like “traffic sign recognition” using complex algorithms distilled from data. A human driver may have a few hundred thousand miles of driving experience over their lifetime but Waymo has covered over 20 million miles on public roads since its creation in 2009 and billions in simulation. In January 2023, Waymo exceeded [one million miles](#) with no human being behind the wheel. With more data to learn from, AI will quickly improve, becoming more adaptive. However, there is still a major concern with AI and autonomous vehicles. The “Trolley” problem is the ethical dilemma where an onlooker can save five lives from a rogue trolley by diverting it to kill just one person. This illustrates why making decisions about who lives and dies are inherently moral judgments but with generative AI — are we now relegating these moral judgments to artificial intelligence that doesn’t have human feeling? AI and human perceptions differ resulting in different kinds of mistakes. As in the pedestrian death caused by a self-driving Uber car, AI can misidentify hazards. How will an autonomous vehicle rationally choose a behavior model in an inevitable collision?

The role of generative AI will only increase as manufacturers continue working toward their goal of producing a fully autonomous Level 5 vehicle. Automotive companies need to ensure the AI tools they utilize in their vehicles comply with safety, data, and privacy regulations. Generative AI is constantly evolving and legal regulatory issues must be taken into consideration.



Consumer Products **AI**

CONSUMER PRODUCTS

The Generative AI Revolution: Key Legal Considerations for the Consumer Products Industry

[Dan Jasnow](#), [Michelle Mancino Marsh](#)

For better or worse, generative artificial intelligence (AI) is already transforming the way we live and work. Within two months of its initial release to the public, ChatGPT reached 100 million monthly active users, making it the fastest-growing consumer application in history. Other popular generative AI tools such as Github Copilot, DALL-E, HarmonAI, and Runway offer powerful tools that can generate computer code, images, songs, and videos, respectively, with limited human involvement. The implications are immense and have already sparked calls for new federal regulatory agencies, a pause on AI development, and even concerns about extinction.

This alert analyzes how AI is already affecting the consumer products industry, as well as some of the key legal considerations that may shape the future of generative AI tools. And [click here to watch our latest Fox Forum](#) as we talk with Mike Pell, the visionary innovation leader at Microsoft, a principal investor in OpenAI and the trailblazing company behind the creation of ChatGPT.

The role of AI in the consumer products industry is multifaceted. Although it raises possible risks for clients, AI's potential to revolutionize the industry has already been realized and will continue to rapidly evolve.

Of significant concern is generative AI's ability to produce new or improved products and the ownership issues for users of the technology. As discussed below, the US Court of Appeals for the Federal Circuit recently held in that according to the plain text of the Patent Act, AI cannot be deemed an inventor.¹ Additionally, the US Copyright Office Review Board [denied](#) copyright protection where the work was wholly generated by AI. Where creators of consumer products integrate generative AI into the design and development process, products may be at risk for lack of IP protection given the current direction of the law.

Despite the risks posed by generative AI, the technology has enhanced consumer experiences while simultaneously optimizing business development and resources. For example, use of AI chatbots to act as online representatives can enhance a customer experience if proper guardrails are employed. These services help users navigate websites and find the products that they are looking for helping to eliminate or minimize friction. Generative AI can also personalize marketing — AI algorithms analyze consumer patterns and advertise products to the portion of the market who is likely to be interested in such products. Similar algorithms can help companies optimize their supply chains by using AI to predict demand and trends, a practice which can lead to less waste and increased sustainability. Additionally, generative AI is being incorporated directly into consumer products — these “smart” devices use AI to adapt and adjust to the preferences and habits of the specific consumer. Despite the beneficial effects on user experience, key issues still exist for consumers when it comes to such AI, including privacy concerns and skepticism regarding AI-generated content.

¹ *Thaler v. Vidal*, 43 F.4th 1207, 1213 (Fed. Cir. 2022).

AI's potential to transform the consumer products industry is already evident, but as the technology continues to advance, companies and consumers should consider other legal issues which we outline below.

1. Accuracy and Reliability

For all their well-deserved accolades and hype, generative AI tools remain a work in progress. Users, especially commercial enterprises, should never assume that AI-created works are accurate, non-infringing, or fit for commercial use. In fact, there have been numerous recorded instances in which generative AI tools have created works that arguably infringe the copyrights of existing works, make up facts, or cite phantom sources. It is also important to note that works created by generative AI may incorporate or display third party trademarks or celebrity likenesses, which generally cannot be used for commercial purposes without appropriate rights or permissions. Like anything else, companies should carefully vet any content produced by generative AI before using it for commercial purposes.

2. Data Security and Confidentiality

Before utilizing generative AI tools, companies should consider whether the specific tools adhere to internal data security and confidentiality standards. Like any third-party software, the security and data processing practices for these tools vary. Some tools may store and use prompts and other information submitted by users. Other tools offer assurances that prompts and other information will be deleted or anonymized. Enterprise AI solutions, such as Azure's OpenAI Service, can also potentially help reduce privacy and data security risks by offering access to popular tools like ChatGPT, DALL-E, Codex, and more within the data security and confidentiality parameters required by the enterprise.

Before authorizing the use of generative AI tools, organizations and their legal counsel should carefully review the applicable [terms of use](#), inquire about access to tools or features that may offer enhanced privacy, security, or confidentiality, and consider whether to limit or restrict access on company networks to any tools that do not satisfy company data security or confidentiality requirements.

3. Software Development and Open-Source Software

One of the most popular use cases for generative AI has been computer coding and software development. But the proliferation of AI tools like GitHub Copilot, as well as a pending lawsuit against its developers, has raised a number of questions for legal counsel about whether use of such tools could expose companies to legal claims or license obligations.

These concerns stem in part from the use of open-source code libraries in the data sets for Copilot and similar tools. While open-source code is generally freely available for use, that does not mean that it may be used without condition or limitation. In fact, open-source code licenses typically impose a variety of obligations on individuals and entities that incorporate open-source code into their works. This may include requiring an attribution notice in the derivative work, providing access to source code, and/or requiring that the derivative work be made available on the same terms as the open-source code.

Many companies, particularly those that develop valuable software products, cannot risk having open-source code inadvertently included in their proprietary products or inadvertently disclosing proprietary code through insecure generative AI coding tools. That said, some AI developers are now providing tools that allow coders to exclude AI-generated code that matches code in large public repositories (in other words, making sure the AI assistant is not directly copying other public code), which would reduce the likelihood of an infringement claim or inclusion of open-source code. As with other AI generated content, users should proceed cautiously, while carefully reviewing and testing AI-contributed code.

4. Content Creation and Fair Compensation

In a recent interview, Billy Corgan, the lead singer of Smashing Pumpkins, [predicted](#) that "AI will change music forever" because once young artists figure out they can use generative AI tools to create new music, they won't spend 10,000 hours in

a basement the way he did. The same could be said for photography, visual art, writing, and other forms of creative expression.

This challenge to the notion of human authorship has ethical and legal implications. For example, generative AI tools have the potential to significantly undermine the IP royalty and licensing regimes that are intended to ensure human creators are fairly compensated for their work. Consider the [recent example](#) of the viral song, “Heart on My Sleeve,” which sounded like a collaboration between Drake and the Weeknd, but was in fact created entirely by AI. Before being removed from streaming services, the song racked up millions of plays—potentially depriving the real artists of royalties they would otherwise have earned from plays of their copyrighted songs. In response, some have suggested that human artists should be compensated when generative AI tools create works that mimic or are closely inspired by copyrighted works and/or that artists should be compensated if their works are used to train the large language models that make generative AI possible. Others have suggested that works should be clearly labeled if they are created by generative AI, so as to distinguish works created by humans from those created by machine.

5. Intellectual Property Protection and Enforcement

Content produced without significant human control and involvement is not protectable by US copyright or patent laws, creating a new orphan class of works with no human author and potentially no usage restrictions. That said, one key principle can go a long way to mitigating IP risk: generative AI tools should aid human creation, not replace it. Provided that generative AI tools are used merely to *help* with drafting or the creative process, then it is more likely that the resulting work product will be protectable under copyright or patent laws. In contrast, asking generative AI tools to create a finished work product, such as asking it to draft an [entire legal brief](#), will likely deprive the final work product of protection under IP laws, not to mention the professional responsibility and ethical implications.

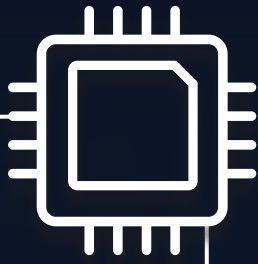
6. Labor and Employment

When Hollywood writers went on strike recently, one issue in particular generated headlines: a demand by the union to regulate the use of artificial intelligence on union projects, including prohibiting AI from writing or re-writing literary material; prohibiting its use as source material; and prohibiting the use of union content to train AI large language models. These demands are likely to presage future battles to maintain the primacy of human labor over cheaper or more efficient AI alternatives. Meanwhile, the Equal Employment Opportunity Commission is [warning](#) companies about the potential adverse impacts of using AI in employment decisions.

7. Future Regulation

Earlier this year, Italy became the first Western country to ban ChatGPT, but it may not be the last. In the US legislators and prominent industry voices have called for proactive federal regulation, including the creation of a new federal agency that would be responsible for evaluating and licensing new AI technology. Others have suggested creating a federal private right of action that would make it easier for consumers to sue AI developers for harm they create. Whether US legislators and regulators can overcome partisan divisions and enact a comprehensive framework seems unlikely, but as is becoming increasingly clear, these are unprecedented times.

Additional research and writing from Natasha Weis, a 2023 summer associate in ArentFox Schiff's New York office and a law student at Fordham University.



Energy & Cleantech **AI**

ENERGY & CLEANTECH

The Generative AI Revolution: Key Impacts to the Environmental & Energy Sectors

[Dan Deeb](#), [Alex Garel-Frantzen](#)

Generative artificial intelligence (AI) is transforming the way we live and work. At its core, AI is the ability of machines to think and learn without encoded commands, mimicking our own cognition. Within two months of its initial release to the public, ChatGPT reached 100 million monthly active users, making it the fastest-growing consumer application in history. Since then, other popular generative AI tools have proliferated with limited human involvement.

AI also has significantly impacted the environmental and energy sectors. US Environmental Protection Agency (EPA) Administrator Michael Regan recently [stated](#) that the Biden Administration will use advanced technologies like AI to decarbonize the economy in an effort to reach its target reduction in greenhouse gas emissions of net zero by 2050. There are several ways in which AI has already influenced the environment and the energy industry. While AI-powered tools are energy-intensive, they can help businesses improve their environmental compliance, optimize energy consumption, reduce waste, develop and implement sustainable practices, enhance the use of renewable energy, and modernize the electricity grid. AI also can be used by litigants to identify potential greenwashing and other claims, transforming how we approach environmental litigation.

1. Energy Usage

We have previously [written](#) about the potentially energy-intensive nature of the Metaverse and cryptocurrency mining. The same can be true for AI tools. Training and operating an AI model requires substantial computational resources which demand considerable amounts of energy. As AI becomes more complex, the models will use even more data and require even more energy. In turn, the focus has increasingly shifted to how all that energy is generated. One study from the University of Massachusetts Amherst [estimated](#) that the carbon footprint of training a single AI natural language processing model is equal to about 300,000 kg of carbon dioxide emissions, equivalent to 125 round-trip flights between New York and Beijing.

Strategies to mitigate the carbon impact of AI include using renewable energy sources to power AI neural networks, producing more efficient graphics processing units, or buying renewable energy credits to offset the carbon produced by AI training and operation.

2. ESG & Greenwashing

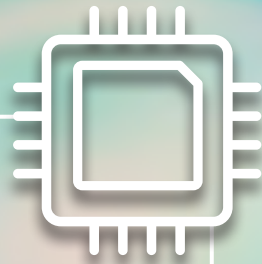
We have also blogged [extensively](#) about the rise in environmental, social, and governance (ESG) considerations, including the SEC's [proposal](#) to require US-registered companies to disclose certain climate-related information, such as energy and water usage and waste production, in their registration statements and annual reports. Concurrently with this focus on ESG has been the rise in [greenwashing cases](#), or litigation targeting corporate statements on environmental impacts or sustainability.

AI is playing a dual role in this space. On the one hand, AI tools are empowering prospective plaintiffs to develop new greenwashing claims. For example, ClimateBert, an AI neural language model, is being used to analyze and fact check corporate reporting and environmental disclosures. According to [ClimateBert](#), it has been pretrained on more than 2 million paragraphs of climate-related texts from various sources, including climate reporting of companies, research articles, and newspapers. Litigants will likely seek to use this and other AI tools to double down on challenging a company's product claims or environmental disclosures.

On the other hand, AI can be used by businesses to optimize energy consumption, reduce waste, and improve sustainability. Based on a survey of 800 industry executives and 300 AI and climate experts, the [Copenhagen Centre on Energy Efficiency](#) published a report in 2020 stating that AI has enabled businesses to decrease their greenhouse gas emissions by 13% and improve power efficiency by 11%. For example, Maximpact is an AI tool that can help monitor, control, evaluate, and manage energy consumption in buildings and factories. It can automate energy usage, identify any problems, and detect equipment failures before they occur. This and other AI tools can analyze large sets of data to monitor and interpret information to optimize energy consumption in real time. AI can also be used to optimize production processes, identify areas of waste, identify potential ways to decrease emissions, and integrate sustainable practices into various industries. For another example, AI-powered farming strategies, like precision agriculture, can automate operations, thereby improving agricultural production sustainability and decreasing the reliance on pesticides.

3. Renewable Energy & Energy Forecasting

Utility companies and the energy sector are likewise turning to AI. Among other things, utilities are leveraging AI to optimize the use of renewable energy sources within their portfolios because AI can improve the reliability of solar and wind power by analyzing massive amounts of meteorological data to help predict when to gather, store, and distribute energy from those sources. Companies like [Nvidia](#) also offer AI-powered solutions to help utilities forecast energy demand, identify real-time outage risks, predict maintenance of system infrastructure, and manage energy supply. Other energy companies are using [AI-powered technologies](#) to provide day-ahead and real-time energy price forecasting for power markets, facilitating strategic decisions related to their power generation assets, and to help further modernize the grid and improve reliability of the system.



Fashion & Retail **AI**

FASHION & RETAIL

The Generative AI Revolution: Key Legal Considerations for the Fashion & Retail Industry

[Anthony V. Lupo](#), [Dan Jasnow](#), [R. Erica Roque](#), [Felicia Xu](#)

For better or worse, generative artificial intelligence (AI) is already transforming the way we live and work. Retail and fashion companies that fail to embrace AI likely risk losing their current market share or, worse, going out of business altogether. This paradigm shift is existential, and businesses that recognize and leverage AI will gain a significant competitive advantage. For instance, some of our clients are using AI to streamline product design processes, reducing the costs and time necessary to generate designs, while others employ virtual models to circumvent issues related to adult and child modeling. Additionally, AI can provide valuable market intelligence to inform sales and distribution strategies. This alert will address these benefits, as well as other significant commercial advantages, and delve into the legal risks associated with utilizing AI in the fashion and retail industry.

There are significant commercial advantages to using AI for retail and fashion companies, including:

1. Product Design

From fast fashion to luxury brands, AI is set to revolutionize the fashion and retail industry. It enables the generation of innovative designs by drawing inspiration from a designer's existing works and incorporating the designer's unique style into new creations. For instance, in March 2023, G-Star Raw created its first denim couture piece designed by AI. We also worked with a client who utilized an AI tool to analyze its footwear designs from the previous two years and generate new designs for 2024. Remarkably, the AI tool produced 50 designs in just four minutes, with half of them being accepted by the company. Typically, this process would have required numerous designers and taken months to complete. While it is unlikely that AI tools will entirely replace human designers, the cost savings and efficiency gained from using such technology are undeniable and should not be overlooked.

2. Virtual Models

2023 marks a groundbreaking year with the world's first AI Fashion Week and the launch of AI-generated campaigns, such as Valentino's Maison Valentino Essentials collection, which combined AI-generated models with actual product photography. Fashion companies allocate a significant portion of their budget to model selection and hiring, necessitating entire departments and grappling with legal concerns such as royalties, SAG, moral issues, and child labor. By leveraging AI tools to create lifelike virtual models, these companies can eliminate the associated challenges and expenses, as AI models are not subject to labor laws — including child entertainment regulations — or collective bargaining agreements.

3. Advertising Campaigns

AI can also be used to create entire advertising campaigns from print copy to email blasts, blog posts, and social media. Companies traditionally invest substantial time and resources in these efforts, but AI can generate such content in mere moments. While human involvement remains essential, AI allows businesses to reduce the manpower required. Retailers can also benefit from AI-powered chatbots, which provide 24/7 customer support while reducing overhead expenses linked to in-person customer service. Moreover, AI's predictive capabilities enable businesses to anticipate trends across various demographics in real-time, driving customer engagement. By processing and analyzing vast amounts of consumer data and preferences, brands can create hyper-personalized and bespoke content, enhancing customer acquisition, engagement, and retention. Furthermore, AI facilitates mass content creation at an impressively low cost, making it an invaluable tool in today's competitive market.

4. ESG –Virtual Mirrors and Apps

From an environmental, social, and corporate governance (ESG) standpoint, the use of AI-powered technology can eliminate the need for retail stores to carry excess inventory, thereby reducing online returns and exchanges. AI smart mirrors can enhance in-store experiences for shoppers by enabling them to virtually try on outfits in various sizes and colors. Furthermore, customers can now enjoy the virtual try-on experience from the comfort of their homes, as demonstrated by Amazon's "Virtual Try-On for Shoes," which allows users to visualize how selected shoes will appear on their feet using their smartphone cameras.

5. Product Distribution and Logistics

Fashion companies rely on their C-level executives to make informed predictions about product quantities, potential sales in specific markets or stores, and the styles that will perform best in each market. In terms of logistics, AI models can be employed to forecast a business's future sales by analyzing historical inventory and sales data. This ability to anticipate supply chain requirements can lead to increased profits and support the industry's initiatives to reduce waste.

To read about additional AI use cases in the fashion industry, [click here](#).

Legal and Ethical Risks

Although AI has some major advantages, it also comes with a number of legal and ethical risks that should be considered, including:

1. Accuracy and Reliability

For all their well-deserved accolades and hype, generative AI tools remain a work in progress. Users, especially commercial enterprises, should never assume that AI-created works are accurate, non-infringing, or fit for commercial use. In fact, there have been numerous recorded instances in which generative AI tools have created works that arguably infringe the copyrights of existing works, make up facts, or cite phantom sources. It is also important to note that works created by generative AI may incorporate or display third-party trademarks or celebrity likenesses, which generally cannot be used for commercial purposes without appropriate rights or permissions. Like anything else, companies should carefully vet any content produced by generative AI before using it for commercial purposes.

2. Data Security and Confidentiality

Before utilizing generative AI tools, companies should consider whether the specific tools adhere to internal data security and confidentiality standards. Like any third-party software, the security and data processing practices for these tools vary. Some tools may store and use prompts and other information submitted by users. Other tools offer assurances that prompts and other information will be deleted or anonymized. Enterprise AI solutions, such as Azure's OpenAI Service, can also potentially help reduce privacy and data security risks by offering access to popular tools like ChatGPT, DALL-E, Codex, and

more within the data security and confidentiality parameters required by the enterprise.

Before authorizing the use of generative AI tools, organizations and their legal counsel should carefully review the applicable [terms of use](#), inquire about access to tools or features that may offer enhanced privacy, security, or confidentiality, and consider whether to limit or restrict access on company networks to any tools that do not satisfy company data security or confidentiality requirements.

3. Software Development and Open-Source Software

One of the most popular use cases for generative AI has been computer coding and software development. But the proliferation of AI tools like GitHub Copilot, as well as a pending lawsuit against its developers, has raised a number of questions for legal counsel about whether use of such tools could expose companies to legal claims or license obligations.

These concerns stem in part from the use of open-source code libraries in the data sets for Copilot and similar tools. While open-source code is generally freely available for use, that does not mean that it may be used without condition or limitation. In fact, open-source code licenses typically impose a variety of obligations on individuals and entities that incorporate open-source code into their works. This may include requiring an attribution notice in the derivative work, providing access to source code, and/or requiring that the derivative work be made available on the same terms as the open-source code.

Many companies, particularly those that develop valuable software products, cannot risk having open-source code inadvertently included in their proprietary products or inadvertently disclosing proprietary code through insecure generative AI coding tools. That said, some AI developers are now providing tools that allow coders to exclude AI-generated code that matches code in large public repositories (in other words, making sure the AI assistant is not directly copying other public code), which would reduce the likelihood of an infringement claim or inclusion of open-source code. As with other AI generated content, users should proceed cautiously, while carefully reviewing and testing AI-contributed code.

4. Content Creation and Fair Compensation

In a recent interview, Billy Corgan, the lead singer of Smashing Pumpkins, [predicted](#) that “AI will change music forever” because once young artists figure out they can use generative AI tools to create new music, they won’t spend 10,000 hours in a basement the way he did. The same could be said for photography, visual art, writing, and other forms of creative expression.

This challenge to the notion of human authorship has ethical and legal implications. For example, generative AI tools have the potential to significantly undermine the IP royalty and licensing regimes that are intended to ensure human creators are fairly compensated for their work. Consider the [recent example](#) of the viral song, “Heart on My Sleeve,” which sounded like a collaboration between Drake and the Weeknd, but was in fact created entirely by AI. Before being removed from streaming services, the song racked up millions of plays — potentially depriving the real artists of royalties they would otherwise have earned from plays of their copyrighted songs. In response, some have suggested that human artists should be compensated when generative AI tools create works that mimic or are closely inspired by copyrighted works and/or that artists should be compensated if their works are used to train the large language models that make generative AI possible. Others have suggested that works should be clearly labeled if they are created by generative AI, so as to distinguish works created by humans from those created by machine.

5. Intellectual Property Protection and Enforcement

Content produced without significant human control and involvement is not protectable by US copyright or patent laws, creating a new orphan class of works with no human author and potentially no usage restrictions. That said, one key principle can go a long way to mitigating IP risk: generative AI tools should aid human creation, not replace it. Provided that generative AI tools are used merely to *help* with drafting or the creative process, then it is more likely that the resulting work product will be protectable under copyright or patent laws. In contrast, asking generative AI tools to create a finished work

product, such as asking it to draft an [entire legal brief](#), will likely deprive the final work product of protection under IP laws, not to mention the professional responsibility and ethical implications.

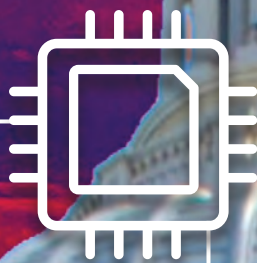
6. Labor and Employment

When Hollywood writers went on strike, one issue in particular generated headlines: a demand by the union to regulate the use of artificial intelligence on union projects, including prohibiting AI from writing or re-writing literary material; prohibiting its use as source material; and prohibiting the use of union content to train AI large language models. These demands are likely to presage future battles to maintain the primacy of human labor over cheaper or more efficient AI alternatives.

Employers are also utilizing automated systems to target job advertisements, recruit applicants, and make hiring decisions. Such systems expose employers to liability if they intentionally or unintentionally exclude or impact protected groups. According to the Equal Employment Opportunity Commission (EEOC), that's precisely what happened with [iTutorGroup, Inc.](#)

7. Future Regulation

Earlier this year, Italy became the first Western country to ban ChatGPT, but it may not be the last. In the United States, legislators and prominent industry voices have called for proactive federal regulation, including the creation of a new federal agency that would be responsible for evaluating and licensing new AI technology. Others have suggested creating a federal private right of action that would make it easier for consumers to sue AI developers for harm they create. Whether US legislators and regulators can overcome partisan divisions and enact a comprehensive framework seems unlikely, but as is becoming increasingly clear, these are unprecedented times.



Government Relations **AI**



GOVERNMENT RELATIONS

Artificial Intelligence: Recent Congressional Activity and a Look to The Future

[Dan Renberg](#), [Oliver Spurgeon](#), [Starshine Chun](#), [Katherine Kramer](#)

In the past few months, the American public has become increasingly fixated on artificial intelligence (AI), especially generative artificial intelligence (GenAI), because of the economic and social considerations associated with this developing technology. AI has inspired contemplation of its potential benefits in the [fight against cancer](#), has become one of the issues in the Hollywood writers' and actors' strikes, has led a group of [tech executives to warn](#) that humans could face extinction from AI, and has led many people to crack jokes, perhaps a bit nervously, about “the robots taking over.”

While many people in business, medicine, and the arts (to name a few) are contemplating how to harness its capabilities, there is increasing interest among Members of Congress to determine whether and how the federal government can and should regulate AI, especially GenAI. One House Member told us that in the past couple of months, “interest in AI at the Member level has gone from zero to 60.” Reflecting the concerns that some policymakers share about GenAI, in one recent Senate hearing, Subcommittee Chairman Sen. Richard Blumenthal (D-CT) [made the case for regulation](#) by creating his own “deepfake” using AI and an AI-generated voice (lifted from his speeches) to deliver an AI-generated opening statement that he developed by asking ChatGPT to draft remarks he would make at the beginning of a hearing on AI. Meanwhile, the House of Representatives took the step of [laying out guidelines](#) for use of ChatGPT by Members and their staffs “for research and evaluation only” at this time.

Given the widespread policy implications of AI, we can expect continued Congressional activity in this area. This alert provides an overview of what the current Congress is doing to educate itself and legislate on topics associated with AI.

For the purposes of this alert, we are using the term “GenAI” to mean the kind of AI that can create new content, like text, images, and video, by learning from pre-existing and publicly available data sources. As our colleagues noted in a [June 7 alert](#) on GenAI and legal considerations for the trade association and nonprofit industry, popular examples of GenAI include Open AI’s ChatGPT, Github Copilot, DALL-E, HarmonAI, and Runway, which can generate computer code, images, songs, and videos, respectively, with limited human involvement.

Congressional Landscape

The environment for Congressional action on AI is hazy at the moment. While there is great interest in the issue, many of the major players in Congress are trying to address very different problems that AI and GenAI will impact in the coming years. Because the universe of issues is so vast, each Member of Congress seems to have his or her own pet priority in this area. For example, on July 13, 50 Democratic Members [wrote the Federal Election Commission](#) (FEC) to express concern about the impact of AI-generated campaign advertisements, particularly those that are fraudulent in nature, and have requested that the FEC begin setting up a framework to regulate AI political ads.

“AI has inspired contemplation of the potential benefits of AI in the fight against cancer, has become one of the factors at issue in the Hollywood writers’ and actors’ strikes, has led a group of tech executives to warn that humans could face extinction from AI, and has led many people to crack jokes, perhaps a bit nervously about ‘the robots taking over.’ Companies, trade associations, and nonprofits with a stake in the AI debate and with particular insight to share should be active at this time, focusing on the Members who are most active and on the multiple committees of jurisdiction.” – Dan Renberg, Government Relations Practice Co-Leader

The national security implications of AI have caught the attention of many in Congress. For example, on April 19, under the leadership of Chairman Joe Manchin (D-WV), the Senate Armed Services Subcommittee on Cybersecurity held a hearing to receive testimony from outside experts and industry leaders on the state of AI and machine learning applications to improve Department of Defense operations. Expert witnesses in Defense AI highlighted the technical challenges – identifying key technologies and integrating them into the system while ensuring that the applications deployed are secure and trusted.

“With enormous stakes for the United States, there is a universal appetite in Washington for regulation of AI but no consensus about AI policy, or the regulatory regime to sustain it. The proposals circulating in Congress are merely the starter’s gun for a debate challenging policymakers and regulators to develop expertise and adapt to rapid tech developments. Key formative decisions about regulatory design are looming that will permanently impact on America’s AI position globally.” – Congressman Phil English, Senior Government Relations Advisor

Others are focused on the impact on consumers and disenfranchised populations. Sen. Jon Ossoff (D-GA) has focused his efforts on protecting human rights and ensuring that people’s civil rights are not violated as AI scrapes the web ([read our recent Privacy Counsel blog post on increasing lawsuits involving data scraping and GenAI tools](#)). Sen. Chris Coons (D-DE) is focused on the impact of AI on patents, trademarks, and the creative economy. At a [June 7 hearing](#), his Senate Subcommittee on Intellectual Property considered questions such as whether, and how, to compensate artists if GenAI creates a song that sounds like Taylor Swift’s music, but is not a sample or carbon copy. At a recent hearing on AI in the same Subcommittee, Sen. Thom Tillis (R-NC) stated that “the creative community is experiencing immediate and acute challenges due to the impact of generative AI.” Others like Sens. Dick Durbin (D-IL) and Lindsey Graham (R-SC) have focused on the need to protect children from adults who create AI-generated child sexual abuse materials by instructing platforms to create child pornography that uses real faces and AI bodies.

Congressman Jay Obernolte (R-CA) has begun to attract attention as a leading expert on AI because of his professional and educational background, which includes an advanced degree in computer science and a former career as a computer programmer. In addition to being Vice Chair of the Congressional Artificial Intelligence Caucus, Rep. Obernolte recently authored an [op-ed column in The Hill](#) in which he provided an overview of multiple policy implications of GenAI, called for industry and government guardrails to prevent misuse of this promising technology, and noted the need to align our nation’s education system with the changes that AI will bring over time.

China’s advancement in AI research and technologies has also been a major focal point of discussion in Congress, especially during AI-related hearings. At a June 22 hearing of the House Science, Space, and Technology Committee, Chairman Frank Lucas (R-OK) stated: “While the United States currently is the global leader in AI research, development, and technology, our adversaries are catching up. The Chinese Communist Party is implementing AI industrial policy at a national scale, investing billions through state-financed investment funds, designating ‘national AI champions,’ and providing preferential tax treatment to grow AI startups. We cannot and should not try to copy China’s playbook. But we can maintain our leadership role in AI, and we can ensure it’s developed with our values of trustworthiness, fairness, and transparency. To do so, Congress needs to make strategic investments, build our workforce, and establish proper safeguards without overregulation.”

“We rely on AI every day. It is navigation for our cars, Siri on our iPhone, robotic vacuum cleaners and so much more. But the advance of AI to develop machines that think, reason, and possess intelligence requires us to understand how we prevent building machines with the capability that would threaten human life. Congress and the Administration are beginning to recognize that there are many policy questions that relate to AI, including

generative artificial intelligence (GenAI) and artificial super intelligence (ASI). Time is short for us to decide how to regulate AI.” – Senator Byron Dorgan, Senior Policy Advisor

There are also big philosophical questions about how and where the government should insert itself in the process of regulating and fostering AI development. Europe has created an “AI sandbox,” where developers can test out their AI products in a safe environment that allows academics to study the harms, impacts, and other implications. In the US, observers have thus far landed in two camps: (1) advocates for creating a new federal agency to regulate AI; or (2) those who prefer to let the private sector innovate and do what scaled the technology to this point. These viewpoints cross party lines and political ideologies at various intersections. Some free-market Republicans have said that the government can use Section 230 of the Communications Decency Act, which has traditionally been used to manage online speech and moderate social media content, to regulate AI. This [set of “small government Republicans” also thinks](#) that there is no need to create a new agency because Section 230 should suffice. On the left, some policymakers are pushing for a new federal agency to collect data on AI and study this issue in detail. One example is the [bill introduced in May](#) by Sens. Michael Bennet (D-CO) and Peter Welch (D-VT) which would establish a Federal Digital Platform Commission that would, among other things, regulate GenAI. This is also the stance of the Biden Administration, which has requested from Congress \$2.6 billion for [the National Artificial Intelligence Research Resource \(NAIRR\) Task Force](#). The Biden Administration also released an [AI Bill of Human Rights](#) last fall, which landed with a thud in Washington among the major players.

At the moment, given the novelty of GenAI and the lack of deep technological understanding among some Members of Congress, there is some confusion about the nature of GenAI and the diverse issues it can create. It is a positive development that on the Senate side, to help bring everyone up to speed, Majority Leader Chuck Schumer (D-NY), Sen. Todd Young (R-IN), and others are holding [three bipartisan briefings for the entire Senate](#) that will feature academics, major industry players, and government officials. Leader Schumer also [laid out a “framework”](#) on June 21 that explained what he intends for the Senate to focus on regarding AI in the coming months. This follows on the heels of an educational session on AI that Speaker Kevin McCarthy (R-CA) held for Members of the House of Representatives earlier this year and private briefings that other groups of House Members have planned for themselves.

It is worth noting that the European Union has been actively working on a regulatory framework for AI, with the European Parliament approving a massive EU AI Act in mid-June that aims to protect the general public from abuses that could arise through the use of AI. [Reactions from US policymakers were mixed](#), with Sen. Michael Bennet (D-CO) commenting, “The United States should be the standard-setter. ... We need to lead that debate globally, and I think we’re behind where the EU is,” while Sen. Mike Rounds (R-SD) indicated that he was not as concerned about falling behind the EU on the regulatory front and was more concerned about continuing to facilitate US dominance in developing new innovations like GenAI.

Conclusion

The nature of AI is such that it will take time for Members of Congress to gain a comfort level with its true potential and what, if any, guardrails are needed. As they increase their familiarity and consult with industry and other stakeholders, it is possible that a consensus will occur and some initial regulatory steps will take place beyond merely introducing bills or holding hearings. As AI dominates public discourse, we can expect a ramping-up of legislative activity. Constituents expressing views – positive or negative – about GenAI when Members are home in their states could also impact the timeline.

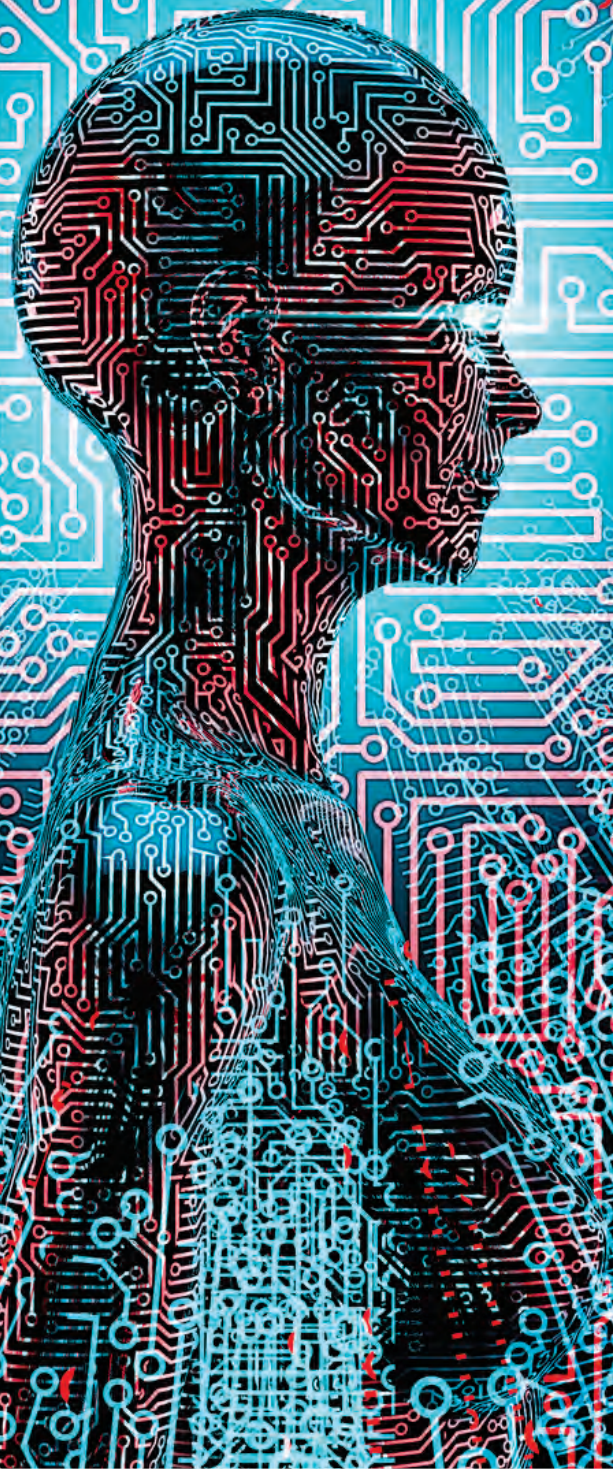
“The legal and policy framework for regulating AI is going to be a front burner issue for Congress and the Administration for some time to come. It is incumbent upon stakeholders with interest in this issue to develop policy principles and recommendations and to convey them to the Hill and relevant agencies.” – Senator Doug Jones, Counsel

It is worth noting that according to a [study by OpenSecrets](#), which tracks money in politics, 123 companies, universities, and trade associations spent a collective \$94 million lobbying the federal government on issues involving AI in the first quarter of 2023. Accordingly, companies, trade associations, and nonprofits with a stake in the AI debate and with particular insight

to share should be active at this time, focusing on the Members who are most engaged with the issues and on the multiple committees of jurisdiction.



Health Care AI



HEALTH CARE

AI's Increasing Role in the Health Care Delivery System: Key Legal Considerations

[Douglas Grimm](#)

No personal services are more important than health care. The use of artificial intelligence (AI), involving machines to perform tasks normally requiring human intelligence, is leading to an expansion of the term “personal.” Recent breakthroughs in generative AI, a type of AI capable of producing natural language, imagery, and audio data, have made the technology increasingly accessible to health care providers.

As AI becomes progressively ingrained in the industry, providers have the opportunity to harness AI to augment the existing care delivery system, and, in some cases, potentially replace existing human processes. This creates a significant necessity to rapidly build regulatory frameworks across the industry to monitor and limit the use of AI.

In a recent [Yale CEO Summit survey](#), 48% of CEOs indicated that AI will have its greatest effect as applied to the health care industry — more than any other industry. This Alert analyzes how AI is already affecting the health care industry, as well as some of the key legal considerations that may shape the future of generative AI tools.

1. The Emerging Regulatory Landscape

Government regulators and medical organizations are already setting guardrails to address the sometimes remarkably unreliable information provided by generative AI platforms. The [American Medical Association](#) recently addressed the issue of medical advice from generative AI chatbots such as ChatGPT and intends to collaborate with the Federal Trade Commission, the Food and Drug Administration, and others to mitigate medical misinformation generated by these tools. It also plans to propose state and federal regulations to address the subject.

Both the [Department of Health and Human Services](#) (HHS) and the [Centers for Medicare and Medicaid Services](#) (CMS) issued “AI Playbooks” to outline their positions on AI technology in accordance with the goals outlined in [Executive Order 13960](#), titled “Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government.” These playbooks are of increasing importance and essential reading for providers contemplating the use and effects of AI.

This government guidance is coming as the health care industry becomes more invested in AI technology. In 2019, the Mayo Clinic entered into a 10-year partnership with Google to bolster the use of cloud computing, data analytics, and machine learning. Four years later, the provider announced plans to utilize Google’s AI Search technology in creating network chat platforms with tailored individual user experience for its physicians and patients. Other companies are in the beginning stages of creating generative AI platforms targeting the health care industry. For example, [Glass Health’s](#) developing platform will utilize a “large language model” (LLM). This consists of deep learning and voluminous data sets to draft health care plans and indicate possible diagnoses for patients based on short or incomplete medical record entries. Health care is one of the initiative’s primary focus areas. The HHS and CMS AI Playbooks should serve as key references during the development of these platforms and initiatives.

2. Offloading the Administrative Burden

One of AI's attractions in the health care industry is its [potential](#) to streamline administrative processes, reduce operating expenses, and increase the amount of time a physician spends with a patient. [Administrative expenses](#) alone account for approximately 15% to 25% of total national health care expenditures in the United States. The [American Academy of Family Physicians](#) reports that the average primary care patient visit lasts approximately 18 minutes, and of that time, 27% is dedicated to direct contact with the patient, whereas 49% is consumed by administrative tasks. Process automation of repetitive tasks, which does not involve AI, has long been part of the patient encounter experience, from appointment scheduling to the revenue cycle management process. Nevertheless, half of all [medical errors](#) in primary care are administrative errors. Deploying AI to initiate intelligent actions has the potential to reduce clerical errors and improve upon those currently-automated processes.

Health care entities are already taking advantage of this emerging technology to increase administrative efficiencies. Transcription services can now be automated using natural language processing and speech recognition, preventing human error and physician burnout—a growing issue discussed in our prior [Alert](#). Health care systems are also applying [algorithms in surgical scheduling](#). An example is the analysis of individual surgeon data to optimize block scheduling of surgical suites, in some cases reducing physician overtime by 10% and increasing space utilization by 19%.

3. Machine Empathy: Androids Dreaming of Electric Sheep

Can AI technology teach providers how to be more empathetic? While Philip K. Dick's 1968 novel, *Do Androids Dream of Electric Sheep?* imagined a dystopian future in which AI was viewed as devoid of empathy, today the potential exists for AI to guide physicians' positive behavior toward their patients. Though currently unconventional, AI has the potential to empower physicians to consider the impact their communications have on patients' lives. With guidance provided by AI technology regarding how to broach difficult subjects, such as terminal illnesses or the death of a loved one, physicians may be able to more confidently and positively interact with others, building a deeper sense of trust with their patients. In the pre-AI world, positive communication behaviors were [shown](#) repeatedly to reduce the likelihood of [litigation](#) and reduce health care costs.

A June 2023 study determined that ChatGPT was not only capable of formulating “thoughtful,” compassionate answers to patient questions or concerns, but in some cases, its answers were preferred over the communications by physicians. The University of California San Diego research study compared responses to patient questions generated by ChatGPT against responses from human physicians, addressing simple ailments up to serious medical concerns. [Feedback](#) from participants indicated that the chatbot answers were rated on average seven times more empathetic than human responses. While machine-manufactured empathy may be anxiety-inducing to many, AI need not replace physicians in conversations requiring clarity and compassion, but rather can serve as a complement to those interactions.

4. “Dr. ChatGPT” – LLMs and A Call to Regulate

Generative AI chat tools may be useful for patients and physicians alike to locate and allocate resources, develop care plans, and diagnose and treat medical conditions. However, as discussed above, the expanding use of these tools in the health care space creates a significant issue: how to know and be confident that these tools are providing reliable information. Is it appropriate at this point in time to utilize these tools for medical purposes? *Doe 1 v. EviCore Healthcare MSI, LLC*

Take, for example, the National Eating Disorder Association's (NEDA) AI-powered LLM chatbot, “Tessa.” Tessa's mission was to promote wellness and provide resources for people affected by eating disorders. However, like [other AI chatbots](#), Tessa's responses were prone to “[hallucinations](#)”—techspeak for a chatbot's inaccurate response. NEDA is not alone in experiencing issues with generative AI-powered chat tools like Tessa. False or misleading information, particularly relating to medical information, leaves users vulnerable and potentially at risk. It is yet to be seen the extent of liability arising from chatbot medical advice, particularly when the chatbot is sponsored by a health care industry organization, but this is undoubtedly within the regulators' sights.

5. Wearable Devices and Privacy Implications

From the invention of the mechanical pedometer in 1780 to current technology capable of detecting medical emergencies and chronic illnesses, wearable devices have become an integral part of today's health care delivery system. The benefits of data derived from the devices cannot be overstated as patient care decisions can now be made with more speed and accuracy. The devices also serve to deepen the physician-patient relationship through more frequent interactions with the provider or staff that drive patient engagement in the care process. The origin of these technologies, however, is rooted in patient data-driven algorithms that range from demographic data to confidential medical information.

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) created national standards to protect patient health information (PHI) from disclosure or use without the patient's consent or knowledge, absent certain exceptions. HIPAA and its corresponding state laws are the first line of defense against threats related to the collection and transmission of sensitive PHI by wearable devices. The Office of Information Security for HHS addressed these concerns in a [September 2022 presentation](#), essential reading for health care data privacy and security experts, that calls for blanket multi-factor authentication, end-to-end encryption, and whole disk encryption to prevent the interception of PHI from wearable devices.

Litigation regarding AI data collection and use has begun. In one case, a recent class action lawsuit in the Northern District of California against OpenAI, the creator of ChatGPT, alleged, among other things, violation of users' privacy rights based on data scraping of social media comments, chat logs, cookies, contact information, login credentials, and financial information. *P.M. v. OpenAI LP*, No. 3:23-cv-03199 (N.D. Cal. filed June 28, 2023). In this context, the ramifications for misuse of PHI is significant.

6. Fraud, Waste, and Abuse Prevention

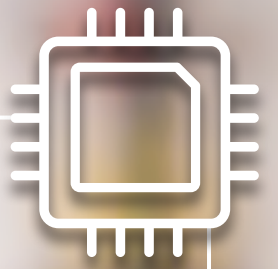
Companies are harnessing AI to detect and prevent fraud, waste, and abuse (FWA) in health care payment systems. [MIT researchers](#) report that insurers indicated a return on FWA systems investment is among the highest of all AI investments. One large health insurer reported a savings of \$1 billion annually through AI-prevented FWA. However, [at least one federal appellate court](#) determined earlier this year that a company's use of AI to provide prior authorization and utilization management services to Medicare Advantage and Medicaid managed care plans is subject to a level of qualitative review that may result in liability for the entity utilizing the AI.

Conclusion

The effect of AI on health care will only continue to grow in scale and scope. New initiatives are announced daily as well as concomitant calls for regulation. Legislators and prominent health care industry voices have called for the creation of a new federal agency that would be responsible for evaluating and licensing new AI technology. Others suggest creation of a federal private right of action that would enable consumers to sue AI developers for harm resulting from the use of AI technology, such as in the OpenAI case discussed above. Whether legislators and regulators can quickly enact a comprehensive framework seems unlikely, but of increasing urgency.

Before utilizing generative AI tools, health care providers should consider whether the specific tools adhere to internal data security and confidentiality standards. Like any third-party software, the security and data processing practices vary. Before implementing the use of generative AI tools, organizations and their legal counsel should (a) carefully review the applicable terms of use, (b) determine whether the tool offers features that enhance data privacy and security, and (c) consider whether to limit or restrict access on company networks to any tools that do not satisfy company data security or confidentiality requirements. It is crucial that these protections be reinforced and augmented quickly because threat proliferation remains a critical issue.

Additional research and writing by Meredith Gillespie, a 2023 summer associate at ArentFox Schiff LLP, Washington, DC's office and a law student at Wake Forest University School of Law.



Hospitality **AI**

HOSPITALITY

The Generative AI Revolution: Key Legal Considerations for the Hospitality Industry

[Dan Jasnow](#), [Kimberly Wachen](#), [Charles Ferguson](#), [Ankit Shrivastava](#)

For better or worse, generative artificial intelligence (AI) is already transforming the way we live and work. Within two months of its initial release to the public, ChatGPT reached 100 million monthly active users, making it the fastest-growing consumer application in history. Other popular generative AI tools such as Github Copilot, DALL-E, HarmonAI, and Runway offer powerful tools that can generate computer code, images, songs, and videos, respectively, with limited human involvement. The implications are immense and have already sparked calls for new federal regulatory agencies, a pause on AI development, and even concerns about extinction.

This alert analyzes how AI is already affecting the Hospitality industry, as well as some of the key legal considerations that may shape the future of generative AI (GenAI) tools. And [click here to watch our latest Fox Forum](#) as we talk with Mike Pell, the visionary innovation leader at Microsoft, a principal investor in OpenAI and the trailblazing company behind the creation of ChatGPT.

The hospitality industry is in its initial phase of adopting AI, and it is already clear that AI has the potential to revolutionize many aspects of hotel operations and customer experience. The industry is now focusing on how to use AI to improve customer experience, automate repetitive tasks, create operational efficiencies, and enhance brand awareness and customer loyalty.

There are many possible applications of how GenAI could affect hotel operations. A GenAI chatbot could take a guest's room service order or serve as a virtual receptionist that could not only fully automate check-in and check-out, but also use a "semantic search" function to answer guest questions, such as, "Where is the best place for coffee near here?" The GenAI chatbot could answer this question by querying a database of options and using the AI technology to find the most similar answer. Another application for GenAI is AI Agents — essentially, the AI is asked to make tasks for itself to complete and is given the ability to interact with a computer to execute those tasks. AI Agents could also be used in a fashion similar to the virtual receptionist mentioned above. Additionally, AI could be a tool to create efficiencies in inventory management, housekeeping room assignments, and maintenance through the use of smart building systems.

At the recent New York University Hospitality Conference, Tim Hentschel, HotelPlanner CEO, provided examples of both positive and negative customer experiences with AI chatbots being used to change reservations. The key difference between experiences was the customer had a more positive experience when a human employee assisted the customer using AI to reduce the wait time versus AI being the sole interface, which can be a frustrating experience. The AI-human hybrid model is much more reliable in the short term than just AI. The risks of hallucinations from GenAI (*i.e.*, when the model creates its own "facts," such as the fake court citations and caselaw references that have recently been in the news) are significant for all industries, including hospitality. Thus, the most likely practical short-term application for GenAI will be to significantly increase the response time for customer support, an analysis which a human employee can then use to provide faster and informed recommendations to hotel customers.

Industry leaders have also discussed using AI to enhance hotel revenue management. By using dynamic pricing models that share information across various assets, hotel managers can optimize prices and bookings to maximize revenue using AI that assesses a variety of factors in real time, such as demand, peak usage, and occupancy rates. Additionally, AI has the potential to personalize pricing to individual guests based upon their past behavior and demographics and identify opportunities for upselling and cross-selling. These features, however, are not without legal risk. Any use of these features that is collusive or otherwise results in price-fixing or discrimination could open the door to a lawsuit.

Intercontinental Hotel Group has recently partnered with Winnow Solutions, with the goal of using AI to reduce the chain's food waste by up to 30%. By connecting the waste bins and inventory systems to AI, hotels should be able to more efficiently and accurately record how quickly and frequently certain items are discarded. Hotel kitchens can use this information to adjust future buying decisions, menus, and food preparation techniques.

Finally, AI may be helpful in assisting hotel owners in analyzing guest feedback and social media posts and providing suggested responses that can be reviewed and edited by hotel staff. AI can also track and analyze guests' booking behaviors, which could assist hotels in creating personalized marketing campaigns targeted at certain customers.

AI is already impacting the guest experience and hospitality companies should consider the legal issues outlined below when deciding how best to use AI in their business.

1. Accuracy and Reliability

For all their well-deserved accolades and hype, GenAI tools remain a work in progress. Users, especially commercial enterprises, should never assume that AI-created works are accurate, non-infringing, or fit for commercial use. In fact, there have been numerous recorded instances in which GenAI tools have created works that arguably infringe the copyrights of existing works, make up facts, or cite phantom sources. It is also important to note that works created by GenAI may incorporate or display third-party trademarks or celebrity likenesses, which generally cannot be used for commercial purposes without appropriate rights or permissions. Like anything else, companies should carefully vet any content produced by GenAI before using it for commercial purposes.

2. Data Security and Confidentiality

Before utilizing GenAI tools, companies should consider whether the specific tools adhere to internal data security and confidentiality standards. Like any third-party software, the security and data processing practices for these tools vary. Some tools may store and use prompts and other information submitted by users. For instance, when you use a GenAI tool, like ChatGPT, you need to send text to the model to get text back (in this instance). OpenAI will keep your prompt unless you tell them otherwise / use the enterprise version. There are a bunch of statistics showing that a lot of confidential information and customer data are being leaked in these prompts by accident from employees who don't know better. It is important to understand how to use GenAI tools so you don't release confidential information. Other tools offer assurances that prompts and other information will be deleted or anonymized. Enterprise AI solutions, such as Azure's OpenAI Service, can also potentially help reduce privacy and data security risks by offering access to popular tools like ChatGPT, DALL-E, Codex, and more within the data security and confidentiality parameters required by the enterprise.

Before authorizing the use of GenAI tools, organizations and their legal counsel should (1) carefully review the applicable terms of use; (2) inquire about access to tools or features that may offer enhanced privacy, security, or confidentiality; and (3) consider whether to limit or restrict access on company networks to any tools that do not satisfy company data security or confidentiality requirements.

3. Software Development and Open-Source Software

One of the most popular use cases for GenAI has been computer coding and software development. But the proliferation of AI tools like GitHub Copilot, as well as a pending lawsuit against its developers, has raised a number of questions for legal counsel about whether use of such tools could expose companies to legal claims or license obligations.

These concerns stem in part from the use of open-source code libraries in the data sets for Copilot and similar tools. While open-source code is generally freely available for use, that does not mean that it may be used without condition or limitation. In fact, open-source code licenses typically impose a variety of obligations on individuals and entities that incorporate open-source code into their works. This may include requiring an attribution notice in the derivative work, providing access to source code, and/or requiring that the derivative work be made available on the same terms as the open-source code.

Many companies, particularly those that develop valuable software products, cannot risk having open-source code inadvertently included in their proprietary products or inadvertently disclosing proprietary code through insecure GenAI coding tools. That said, some AI developers are now providing tools that allow coders to exclude AI-generated code that matches code in large public repositories (in other words, making sure the AI assistant is not directly copying other public code), which would reduce the likelihood of an infringement claim or inclusion of open-source code. As with other AI generated content, users should proceed cautiously, while carefully reviewing and testing AI-contributed code.

4. Content Creation and Fair Compensation

In a recent interview, Billy Corgan, the lead singer of Smashing Pumpkins, [predicted](#) that “AI will change music forever” because once young artists figure out they can use GenAI tools to create new music, they won’t spend 10,000 hours in a basement the way he did. The same could be said for photography, visual art, writing, and other forms of creative expression.

This challenge to the notion of human authorship has ethical and legal implications. For example, GenAI tools have the potential to significantly undermine the intellectual property (IP) royalty and licensing regimes that are intended to ensure human creators are fairly compensated for their work. Consider the [recent example](#) of the viral song, “Heart on My Sleeve,” which sounded like a collaboration between Drake and the Weeknd, but was in fact created entirely by AI. Before being removed from streaming services, the song racked up millions of plays — potentially depriving the real artists of royalties they would otherwise have earned from plays of their copyrighted songs. In response, some have suggested that human artists should be compensated when GenAI tools create works that mimic or are closely inspired by copyrighted works and/or that artists should be compensated if their works are used to train the large language models that make GenAI possible. Others have suggested that works should be clearly labeled if they are created by GenAI, so as to distinguish works created by humans from those created by machine.

5. Intellectual Property Protection and Enforcement

Content produced without significant human control and involvement is not protectable by US copyright or patent laws, creating a new orphan class of works with no human author and potentially no usage restrictions. That said, one key principle can go a long way to mitigating IP risk: GenAI tools should aid human creation, not replace it. Provided that GenAI tools are used merely to *help* with drafting or the creative process, then it is more likely that the resulting work product will be protectable under copyright or patent laws. In contrast, asking GenAI tools to create a finished work product, such as asking it to draft an [entire legal brief](#), will likely deprive the final work product of protection under IP laws, not to mention the professional responsibility and ethical implications.

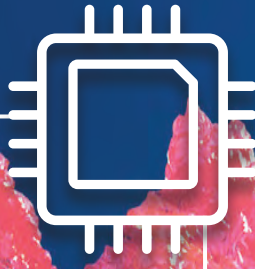
6. Labor and Employment

When the Writers Guild of America recently went on strike, one issue in particular generated headlines: a demand by the union to regulate the use of AI on union projects, including prohibiting AI from writing or re-writing literary material; prohibiting its use as source material; and prohibiting the use of union content to train large AI language models. These demands are likely to presage future battles to maintain the primacy of human labor over cheaper or more efficient AI alternatives. Meanwhile, the Equal Employment Opportunity Commission (EEOC) is [warning](#) companies about the potential adverse impacts of using AI in employment decisions.

7. Future Regulation

Earlier this year, Italy became the first Western country to ban ChatGPT, but it may not be the last. In the US legislators and prominent industry voices have called for proactive federal regulation, including the creation of a new federal agency that would be responsible for evaluating and licensing new AI technology. Others have suggested creating a federal private right of action that would make it easier for consumers to sue AI developers for harm they create. Whether US legislators and regulators can overcome partisan divisions and enact a comprehensive framework seems unlikely, but as is becoming increasingly clear, these are unprecedented times.

Life Sciences AI



LIFE SCIENCES

Legal Implications of AI in the Life Sciences Industry

[Richard Berman](#), [Jeannette McLaughlin](#), [Sailesh Patel](#), [Matthew Wilkerson](#)

Artificial intelligence (AI) is rapidly transforming the life sciences industry, with significant advancements in various areas. These innovations bring new legal challenges related to intellectual property, data protection, regulatory compliance, and ethical considerations that stakeholders must address.

1. Drug Discovery and Development

AI algorithms can streamline drug discovery by analyzing large data sets to identify potential drug candidates, predict their effectiveness, and optimize their chemical structures. The use of AI in this area raises legal questions regarding patent eligibility, ownership of AI-generated inventions, and potential liability issues in cases of adverse effects from AI-generated drugs. Regulatory agencies may need to establish guidelines for AI-guided product development and address these concerns to promote safe, effective, and responsible innovation.

2. Precision Medicine and Personalized Treatments

AI can help identify the most effective treatments for individual patients by analyzing patient data, such as genetic information and medical records. This may enable improved outcomes and reduced side effects. However, the use of AI in this area must comply with applicable privacy and data protection laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR), ensuring the confidentiality, integrity, and proper consent for the use of personal health information. Companies must implement robust data protection measures and technologies to maintain consumer trust, comply with regulatory requirements, and prevent potential breaches.

3. Medical Imaging and Diagnostics

AI-powered tools can analyze medical images, such as X-rays and MRIs, leading to faster and more accurate diagnoses. AI-based diagnostic tools must adhere to medical device regulations and obtain necessary approvals from organizations like the US Food and Drug Administration (FDA) and the European Medicines Agency (EMA). Additionally, the use of AI in diagnostics raises questions about liability in cases of misdiagnosis or failure to diagnose conditions accurately. It would be helpful for legal professionals and industry to collaborate to establish clear guidelines for assigning responsibility in such cases.

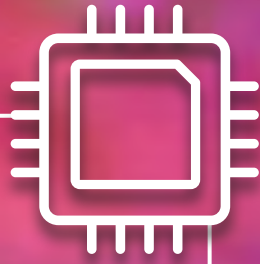
4. Disease Prediction and Prevention

AI can analyze large data sets from various sources, such as electronic health records and wearable devices, to identify risk factors and predict the likelihood of developing certain diseases. Legal considerations in this area include patient privacy, informed consent, and potential discrimination based on genetic information. AI systems must comply with data protection regulations and ensure that predictive analyses do not unfairly disadvantage individuals based on their health data. Policymakers may need to develop new regulations to address potential ethical issues arising from predictive health analytics.

5. Clinical Trials and Research

AI can streamline the clinical trial process by identifying suitable candidates for trials, improving access to trials, optimizing trial designs, and analyzing trial data more efficiently. AI can also help researchers identify patterns and trends in existing data, leading to new hypotheses and avenues for investigation. The use of AI in clinical trials introduces legal concerns related to patient consent, data protection, and the ethical use of AI in research. Regulatory agencies are establishing guidelines for AI's role in trial design, participant selection, and data analysis, ensuring the protection of human subjects and the integrity of scientific research.

In conclusion, as AI continues to revolutionize the life sciences industry, it is crucial for legal professionals, researchers, and companies to be aware of these legal implications and work together to ensure the responsible and ethical development and application of AI technologies. By addressing these challenges, the life sciences industry can harness the full potential of AI to improve patient care, advance scientific research, and drive innovation.



Long Term Care & Senior Living **AI**



LONG TERM CARE & SENIOR LIVING

The Generative AI Revolution: Key Legal Considerations for the Long Term Care and Senior Living Industry

[Dan Jasnow](#), [Jo-Ann Marchica](#), [Mindy Pittell Hurwitz](#), [Stephen Blake](#)

For better or worse, generative artificial intelligence (AI) is already transforming the way we live and work. Within two months of its initial release to the public, ChatGPT reached 100 million monthly active users, making it at the time the fastest-growing consumer application in history. ChatGPT and other popular generative AI tools such as Github Copilot, DALL-E, HarmonAI, and Runway offer powerful instruments that can generate computer code, audio, and videos with limited human involvement. The implications are immense and have sparked calls for new federal regulatory agencies and a pause on AI development. There have even been concerns about extinction.

This alert analyzes how AI is already affecting the long term care and senior living industry, as well as some of the key legal considerations that may shape the future of generative AI tools.

While the impact artificial intelligence will have on the long term care and senior living industry is tied closely with the impact on the [health care industry](#) as a whole, certain niche areas specifically impact both institutional and home care settings. With respect to care, generative AI technology can help provide medication and meal reminders for seniors. Certain wearables can help care staff or caregivers monitor signs of a potential fall, changes in vital systems, and disrupted sleep patterns. Yet, the benefits go beyond just residents or patients. Whether providing care or not, family members will benefit greatly from generative AI as they can stay better updated about the care of their loved ones. As with all new technology, the benefits must be weighed against concerns surrounding accuracy and privacy, as is addressed in more detail below.

1. Accuracy and Reliability

For all their well-deserved accolades and hype, generative AI tools remain a work in progress, but getting it wrong in the long term care and senior living space can have significant consequences. Operators that utilize generative AI to assist in operations need to ensure that electronic health records are accurate and reliable. For example, if an inaccurate assessment is completed for a potential new resident, such an error can lead to significant gaps in that resident's care. Additionally, documentation errors for things such as medications can lead not only to harm to the resident, but such errors can also result in state survey violations.

2. Data Security and Confidentiality

Before utilizing generative AI tools, companies should consider whether the specific tools adhere to internal data security and confidentiality standards and, for some operators, whether the tools adhere to federal and state health privacy and security standards. Like any third-party software, these tools' security and data processing practices vary. Some devices may

store and use prompts and other information submitted by users. Other tools offer assurances that prompt and other information will be deleted or anonymized. Enterprise AI solutions, such as Azure's OpenAI Service, can also potentially help reduce privacy and data security risks by offering access to popular tools like ChatGPT, DALL-E, Codex, and more within the data security and confidentiality parameters required by the enterprise.

Before authorizing the use of generative AI tools, owners and operators, along with their legal counsel should (i) carefully review the applicable terms of use, (ii) inquire about access to tools or features that may offer enhanced privacy, security, or confidentiality, and (iii) consider whether to limit or restrict access on company networks to any tools that do not satisfy company data security or confidentiality requirements.

3. Intellectual Property Protection and Enforcement

Content produced without significant human control and involvement is not protectable by US copyright or patent laws, creating a new orphan class of works with no human author and potentially no usage restrictions. That said, one key principle can go a long way to mitigating IP risk: generative AI tools should aid human creation, not replace it. Provided that generative AI tools are used merely to help with drafting or the creative process, then it is more likely that the resulting work product will be protectable under copyright or patent laws. In contrast, asking generative AI tools to create a finished work product, such as asking it to draft an [entire legal brief](#), will likely deprive the final work product of protection under IP laws, not to mention the professional responsibility and ethical implications.

For long term care and senior living, it is easy to imagine a new operator using generative AI tools to develop policies and procedures, assessment forms, or even Residency Agreements in accordance with state requirements. These items are protected IP and require human creation.

4. Labor and Employment

When Hollywood writers went on strike recently, one issue in particular generated headlines: a demand by the union to regulate the use of artificial intelligence on union projects, including prohibiting AI from writing or re-writing literary material; prohibiting its use as source material; and prohibiting the use of union content to train AI large language models. These demands are likely to presage future battles to maintain the primacy of human labor over cheaper or more efficient AI alternatives. Meanwhile, the Equal Employment Opportunity Commission is [warning](#) companies about the potential adverse impacts of using AI in employment decisions.

For long term care and senior living, the rise of generative AI may actually be seen as a benefit to combat staffing shortages. There are many tools already available that cut down on the time spent on administrative tasks. This "extra" time will allow care staff to spend more time providing care and monitoring patients and can help facilities overcome staffing shortages that have been impacting the industry for some time now.

5. Intellectual Property Protection and Enforcement

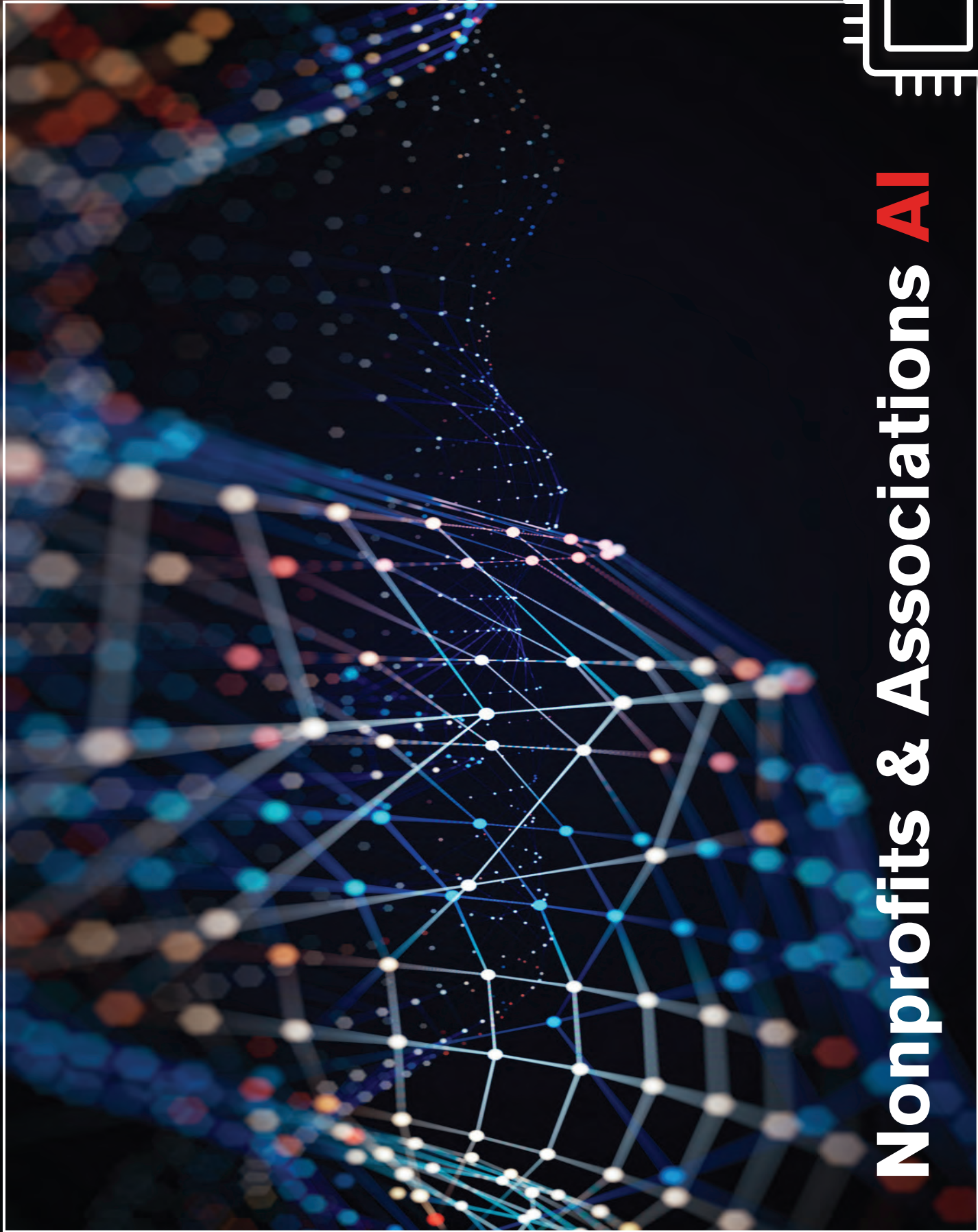
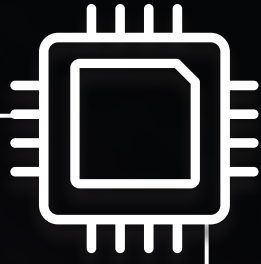
Content produced without significant human control and involvement is not protectable by US copyright or patent laws, creating a new orphan class of works with no human author and potentially no usage restrictions. That said, one key principle can go a long way to mitigating IP risk: GenAI tools should aid human creation, not replace it. Provided that GenAI tools are used merely to *help* with drafting or the creative process, then it is more likely that the resulting work product will be protectable under copyright or patent laws. In contrast, asking GenAI tools to create a finished work product, such as asking it to draft an [entire legal brief](#), will likely deprive the final work product of protection under IP laws, not to mention the professional responsibility and ethical implications.

6. Future Regulation

Earlier this year, Italy became the first Western country to ban ChatGPT, but it may not be the last. In the US, legislators and prominent industry voices have called for proactive federal regulation, including creating a new federal agency responsible for evaluating and licensing new AI technology. Others have suggested creating a federal private right of action that would make it easier for consumers to sue AI developers for harm they create. Whether US legislators and regulators can overcome partisan divisions and enact a comprehensive framework seems unlikely, but as is becoming increasingly clear, these are unprecedented times.

For long term care and senior living, one potential challenge will be whether state licensing agencies are comfortable not only with the technology that is used, but also the policies and procedures that are developed regarding the use of generative AI. While many states do encourage innovative methods of care, operators must be sure the new technology that they intend to implement does not run afoul of any state-specific restrictions.

Nonprofits & Associations **AI**



NONPROFIT & ASSOCIATIONS

The Generative AI Revolution: Key Legal Considerations for the Nonprofit & Trade Association Industry

[Dan Jasnow](#), [Brian Schneider](#), [Sean Glynn](#)

Generative artificial intelligence (AI) is already transforming the way we live and work. Within two months of its initial release to the public, ChatGPT reached 100 million monthly active users, making it the fastest-growing consumer application in history. Other popular generative AI tools such as Github Copilot, DALL-E, HarmonAI, and Runway offer powerful tools that can generate computer code, images, songs, and videos, respectively, with limited human involvement. The implications are immense and have already sparked calls for new federal regulatory agencies, a pause on AI development, and even concerns about extinction.

This alert describes how AI is already affecting the nonprofits and associations industry, as well as some of the key legal considerations that may shape the future of generative AI tools. And [click here to watch our latest Fox Forum](#) as we talk with Mike Pell, the visionary innovation leader at Microsoft, a principal investor in OpenAI and the trailblazing company behind the creation of ChatGPT.

For nonprofits and trade associations, our clients already are starting to use AI tools like ChatGPT to create marketing communications, member messages, and stunning graphics. We've also seen them use AI to identify and summarize competitors' and members' business operations for planning purposes and to create mission and vision statement drafts for strategic planning sessions.

Below, we outline key legal issues organizations should keep in mind.

1. Accuracy and Reliability

For all their well-deserved accolades and hype, generative AI tools remain a work in progress. Users should never assume that AI-created works are accurate, non-infringing, or fit for an organization's use. In fact, there have been numerous recorded instances in which generative AI tools have created works that arguably infringe the copyrights of existing works, make up facts, or cite phantom sources. It is also important to note that works created by generative AI may incorporate or display third-party trademarks or celebrity likenesses, which generally cannot be used for an organization's purposes without appropriate rights or permissions. Like anything else, organizations should carefully vet any content produced by generative AI before using it for your organization.

2. Data Security and Confidentiality

Before utilizing generative AI tools, organizations should consider whether the specific tools adhere to internal data security and confidentiality standards. Like any third-party software, the security and data processing practices for these tools vary. Some tools may store and use prompts and other information submitted by users. Other tools offer assurances that prompts and other information will be deleted or anonymized. Enterprise AI solutions, such as Azure's OpenAI Service, can also potentially help reduce privacy and data security risks by offering access to popular tools like ChatGPT, DALL-E, Codex, and more within the data security and confidentiality parameters required by the enterprise.

Before authorizing the use of generative AI tools, organizations and their legal counsel should carefully review the applicable terms of use, inquire about access to tools or features that may offer enhanced privacy, security, or confidentiality, and consider whether to limit or restrict access on organization networks to any tools that do not satisfy the organization's data security or confidentiality requirements.

3. Software Development and Open-Source Software

One of the most popular use cases for generative AI has been computer coding and software development. But the proliferation of AI tools like GitHub Copilot, as well as a pending lawsuit against its developers, has raised a number of questions for legal counsel about whether use of such tools could expose companies and organizations to legal claims or license obligations.

These concerns stem in part from the use of open-source code libraries in the data sets for Copilot and similar tools. While open-source code is generally freely available for use, that does not mean that it may be used without condition or limitation. In fact, open-source code licenses typically impose a variety of obligations on individuals and entities that incorporate open-source code into their works. This may include requiring an attribution notice in the derivative work, providing access to source code, and/or requiring that the derivative work be made available on the same terms as the open-source code.

Many companies and organizations, particularly those that develop valuable software products, cannot risk having open-source code inadvertently included in their proprietary products or inadvertently disclosing proprietary code through insecure generative AI coding tools. That said, some AI developers are now providing tools that allow coders to exclude AI-generated code that matches code in large public repositories (in other words, making sure the AI assistant is not directly copying other public code), which would reduce the likelihood of an infringement claim or inclusion of open-source code. As with other AI-generated content, users should proceed cautiously, while carefully reviewing and testing AI-contributed code.

4. Content Creation and Fair Compensation

In a recent interview, Billy Corgan, the lead singer of Smashing Pumpkins, [predicted](#) that "AI will change music forever" because once young artists figure out they can use generative AI tools to create new music, they won't spend 10,000 hours in a basement the way he did. The same could be said for photography, visual art, writing, and other forms of creative expression.

This challenge to the notion of human authorship has ethical and legal implications. For example, generative AI tools have the potential to significantly undermine the IP royalty and licensing regimes that are intended to ensure human creators are fairly compensated for their work. Consider the [recent example](#) of the viral song "Heart on My Sleeve," which sounded like a collaboration between Drake and the Weeknd but was in fact created entirely by AI. Before being removed from streaming services, the song racked up millions of plays – potentially depriving the real artists of royalties they would otherwise have earned from plays of their copyrighted songs. In response, some have suggested that human artists should be compensated when generative AI tools create works that mimic or are closely inspired by copyrighted works and/or that artists should be compensated if their works are used to train the large language models that make generative AI possible. Others have

suggested that works should be clearly labeled if they are created by generative AI, so as to distinguish works created by humans from those created by machine.

5. Intellectual Property Protection and Enforcement

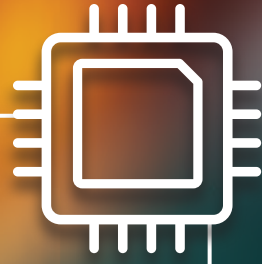
Content produced without significant human control and involvement is not protectable by US copyright or patent laws, creating a new orphan class of works with no human author and potentially no usage restrictions. That said, one key principle can go a long way to mitigating IP risk: generative AI tools should aid human creation, not replace it. Provided that generative AI tools are used merely to *help* with drafting or the creative process, then it is more likely that the resulting work product will be protectable under copyright or patent laws. In contrast, asking generative AI tools to create a finished work product, such as asking a tool to draft an [entire legal brief](#), will likely deprive the final work product of protection under IP laws, not to mention the professional responsibility and ethical implications.

6. Labor and Employment

When Hollywood writers went on strike, one issue in particular generated headlines: a demand by the union to regulate the use of artificial intelligence on union projects, including prohibiting AI from writing or re-writing literary material; prohibiting its use as source material; and prohibiting the use of union content to train AI large language models. These demands are likely to presage future battles to maintain the primacy of human labor over cheaper or more efficient AI alternatives. Meanwhile, the Equal Employment Opportunity Commission (EEOC) is [warning](#) companies about the potential adverse impacts of using AI in employment decisions.

7. Future Regulation

Earlier this year, Italy became the first Western country to ban ChatGPT, but it may not be the last. In the United States, legislators and prominent industry voices have called for proactive federal regulation, including the creation of a new federal agency that would be responsible for evaluating and licensing new AI technology. Others have suggested creating a federal private right of action that would make it easier for consumers to sue AI developers for harm they create. Whether US legislators and regulators can overcome partisan divisions and enact a comprehensive framework seems unlikely, but as is becoming increasingly clear, these are unprecedented times.



Privacy, Data Protection & Data Security **AI**



PRIVACY, DATA PROTECTION & DATA SECURITY

Generative Artificial Intelligence, Data Minimization, and the Gold Rush of the Early 2020s

[D. Reed Freeman, Jr.](#)

In the United States, the principle of data minimization is embedded firmly within the Federal Trade Commission (FTC) Act, through FTC enforcement activities, and in the host of state-level privacy laws and rules that have proliferated in recent years.

The explosive emergence in recent months of commercial applications of generative artificial intelligence (GenAI) technology and tools, and their need to train on very large data sets, and to continue to develop on user-generated data supplied in GenAI prompts (prompt data) presents some challenges in applying this principle.

Now is the time to take stock of your data minimization strategies to ensure that your technology and tools based on GenAI are resilient, can withstand regulatory scrutiny, and can position your organization to compete effectively in a market estimated to experience a compound annual growth rate of over 35% through 2030 – more than 10 times higher than the rate of the US economy.¹

Data Minimization Laws

In general, the data minimization principle holds that controllers should only collect and process the personal information they need to accomplish a disclosed purpose, or a contextually compatible purpose, should only transfer such data consistent with those purposes, and should only maintain personal information as long as is necessary for those purposes.

FTC Act

The FTC's enforcement posture has changed dramatically over the past 11 years. As far back as 2012, the FTC has advocated "reasonable collection limitation."² Now, according to the FTC, using an interface to steer consumers to an option to provide more information than the context makes necessary may be considered a "dark pattern," in violation of Section 5.³ Focusing more narrowly on AI and machine learning in a recent case, all three sitting Commissioners stated that "machine learning is no excuse to break the law. Claims from businesses that data must be indefinitely retained to improve algorithms do not override legal bans on indefinite retention of data. The data you use to improve your algorithms must be lawfully collected and lawfully retained." In a clear warning shot far beyond the contours of the case at hand, the FTC continued, "companies

¹ Compare Generative AI Market Size To Reach \$109.37 Billion By 2030, Grand View Research (May 2023), available at <https://www.grandviewresearch.com/press-release/global-generative-ai-market> with The Economic Outlook for 2023 to 2033 in 16 Charts, Congressional Budget Office (February 2023), available at <https://www.cbo.gov/publication/58880>.

² See FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

³ FTC Staff Report, Bringing Dark Patterns to Light, available at https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%2009.14.2022%20-%20FINAL.pdf.

would do well to heed this lesson.”⁴

The FTC’s Commercial Surveillance Advanced Notice of Proposed Rulemaking makes clear that the FTC is considering codifying data minimization into federal law.⁵ In the meantime, the FTC has already brought a number of enforcement actions focused on data minimization. These cases allege that companies violated laws enforced by the FTC when they:

- collected more personal information than they disclose or need for the purposes for which it was collected;⁶
- used⁷ or shared⁸ personal information for incompatible purposes; or
- retained the information in violation of their own representations, or beyond the period for which the data is required for the purposes for which it was collected.⁹

US State Laws

The California Privacy Protection Act, as amended by the California Privacy Rights Act, was the first comprehensive privacy law in the United States to reduce the data minimization principle to codified law. Collection of personal information must be proportionate to the purpose for which it was collected or reasonably necessary for another purpose, provided that purpose is compatible with the context of collection.¹⁰ New laws taking effect this year in Colorado,¹¹ Connecticut,¹² Virginia,¹³ and laws passed this legislative cycle that take effect in 2024 and beyond in Indiana,¹⁴ Iowa,¹⁵ Tennessee,¹⁶ Montana,¹⁷ and Texas¹⁸ all share common principles. In short, it is now black-letter law in the United States that personal information can only be collected for disclosed and contextually relevant purposes.

⁴ Statement of Commissioner Alvaro M. Bedoya Joined by Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter In *United States v. Amazon.com, Inc.* (May 31, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya-Statement-on-Alexa-Joined-by-LK-and-RKS-Final-1233pm.pdf.

⁵ <https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf> at p. 51284 (Q.43)

⁶ *United States v. Edmodo, LLC*, available at https://www.ftc.gov/system/files/ftc_gov/pdf/edmodocomplaintfiled.pdf.

⁷ In the Matter of Support King, LLC, available at https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfonecomplaint_o.pdf.

⁸ In the Matter of Goldenshores Technologies, LLC, and Erik M. Geidl, Complaint, available at <https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf>, see also, e.g., *United States v. Easy Healthcare Corp.*, available at https://www.ftc.gov/system/files/ftc_gov/pdf/2023186easyhealthcarecomplaint.pdf, In the Matter of Flo Health, Inc., available at https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.

⁹ In the Matter of Everalbum, Inc., available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint_final.pdf.

¹⁰ Cal. Civ. Code § 1798.100 (“A business’ collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.”)

¹¹ Co. Rev. Statutes § 6-1-1304(4)(a)-(b), available at https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

¹² Connecticut Act Concerning Personal Data Privacy and Online Monitoring § 10(f), available at <https://www.cga.ct.gov/2022/act/pa/pdf/2022PA-00015-RooSB-00006-PA.pdf>.

¹³ Virginia Code Ann. §59.1-578, available at <https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-578/>

¹⁴ Indiana Consumer Data Protection Act, Ch. 4, § 1 available at <https://iga.in.gov/legislative/2023/bills/senate/5#document-8806200c>.

¹⁵ Iowa SF 262 § 7(6), available at <https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF%20262>.

¹⁶ Tenn. Code Ann. § 47-18-3204, available at <https://www.capitol.tn.gov/Bills/113/Bill/SB0073.pdf>.

¹⁷ Montana Consumer Data Privacy Act, § 7, available at <https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf>.

¹⁸ Tx. Bus. and Prof. Code 11-541-101, available at <https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00004F.pdf#navpanes=0>.

GenAI

Two aspects of GenAI require attention when considering data minimization. First, GenAI technology requires an extraordinary amount of training data to be useful. Much of this data is scraped from websites and much of it contains personal or sensitive personal information. Second, both the underlying GenAI technology and commercial tools using it continue to train on prompt data, which may also contain personal or sensitive personal information.

Companies around the world are now scrambling to license commercial GenAI technology to introduce all manner of tools to their customers. By heeding these steps, organizations can meet their data minimization requirements for compliance and risk-reduction purposes and, having done so, will be poised to capture their part of the expansive new GenAI market.

Contracts

One risk associated with licensing GenAI technology is that it may have been trained on data sets including personal information or sensitive personal information — or both. Companies can limit their risk in this regard by focusing their attention on the representations, warranties, limitations of liability, and indemnity provisions. In the GenAI context, these terms are not yet standard. The market is still developing. But savvy organizations are familiar with risk shifting. Don't let the rush-to-market period we're in now expose your organization to undue risk. Regulators have shown a willingness to seek algorithmic disgorgement — the death penalty that could cripple your GenAI rollout — for algorithms based on data improperly collected.¹⁹ Do your best to make sure that you're building your tool on a solid foundation and that you're protected against downside risk.

What about prompt data? Consider whether this data will go to the GenAI technology developer itself, and for what purposes? Will it be used to continue the development of the tool just for your organization or for others as well? If the toolmaker will use the data just for you, can the toolmaker be your service provider or processor just for this purpose? Appropriate data processor or service provider agreements under the new state laws may get your organization some control over the further use and disclosure of user prompt data and limit your risk to that extent. Your processor/service agreement should define the uses to which the GenAI technology developer will make of prompt data and should be parallel with the purposes you disclose at the point of collection and in your privacy policy. You should also make sure that the toolmaker is equipped to assist you in responding to consumer rights requests.

Your Disclosures – Proximate to the Prompt and Privacy Policy

Because privacy laws place an emphasis on disclosed and contextually relevant purposes, it is critical to have clear and conspicuous disclosures proximate to the prompt field. These disclosures should make clear that data submitted as a GenAI prompt will be used by your organization and (if applicable) the AI technology developer to generate content and to train the tool (and, if applicable, the underlying GenAI technology) on an ongoing basis. The company's privacy policy should also contain the same disclosures. They should also explain that the user may prevent this use by not entering any personal information into the prompt field. If possible, end users should have an opportunity to opt-out of the processing of prompt data for further development of the GenAI tool and the underlying technology. But before you offer that, be sure you can honor it.

De-Identifying Prompt Data

Because GenAI's fuel is data, and because of the expansive definition of "personal information" and "personal data" in the state privacy laws, it may not be feasible over time to sort through all your organization's prompt data to delete all personal information before the data is used for GenAI product development. But what about de-identification? California's

¹⁹ United States v. Kurbo, Stipulated Order (March 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/wwkurbostipulatedorder.pdf.

Consumer Privacy Act (CCPA) excludes de-identified data²⁰ and contains a typical standard that organizations must meet to enjoy this protection, borrowed from Federal Trade Commission enforcement and policy work.

Section 1798.140(m) of the CCPA defines “deidentified” as:

information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

- (1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.
- (2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.
- (3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.²¹

Well-known work by NIST²² and HHS²³ serves as tactical guideposts. The point is to do what you can to maintain the volume of data needed to develop GenAI tools while avoiding data minimization risks associated with prompt data.

Conclusion

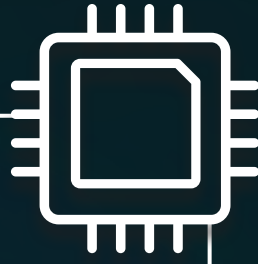
Privacy law has long wrestled with the urge to collect and keep data for future use. What’s new is that with GenAI, what was once a question of “I may want to use the data in the future” has now become “I will need to use the data in the future.” Data minimization standards do not act as a ban on the use of training data and prompt data for the development of commercial GenAI technology and tools. In fact, done with care, you can use data minimization standards as both a shield to avoid regulatory scrutiny and as a sword to distinguish your GenAI tools from others in an almost limitless market. of ChatGPT.

²⁰ Cal. Civ. Code § 1798.140(v)(3).

²¹ Cal. Civ. Code § 1798.140(m).

²² See NISTIR 8053, available at <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>.

²³ HHS, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, available at <https://www.hhs.gov/guidance/document/guidance-regarding-methods-de-identification-protected-health-information-accordance-o>.



Private Companies **AI**

PRIVATE COMPANIES

Artificial Intelligence in the Family Office: Risks and Rewards

[Sarah Severson](#), [Matt Galo](#)

Generative artificial intelligence (AI) is computer software that can create new content or data by tracking patterns from existing data. AI is dominating public discourse: across all media, all industries, and all segments of the population. Whether you are an individual looking to enhance safety or efficiency at home or a business owner seeking to lower overhead and improve efficiency, it seems no one is immune from asking: how can AI work for me?

AI has arrived in the family office space and is already changing the legal and administrative procedures used by family offices. Attorneys and family office teams naturally are curious how these new technologies can streamline and improve their practices, but they also would be wise to consider potential risks related to its use as we outline here.

Potential Uses and Rewards

Document Drafting

Generative AI tools may be particularly helpful for document drafting. Large language models (LLMs) can provide a meaningful draft of anything from an engagement letter to a comprehensive will and trust. Professionals using AI drafting capabilities should *not* treat any AI-produced document as a final draft. LLMs are still a work-in-progress, and any AI-created material should be thoroughly reviewed and edited prior to use.

Estate Summarization

Generative AI may also be useful in reviewing complex estate documents and asset compilations. Based on initial documents and information provided by the client, a family office professional or an attorney may be able to use AI as a quasi-search engine. Questions could be as simple as “What is the net worth of this client?” or as complex as “Would this client benefit from setting up a GRAT or sale to an Intentionally Defective Grantor Trust?” While AI used in this fashion has the potential to save significant time, the user would need to have a high level of confidence in the AI software before relying on it for answers to more complex questions.

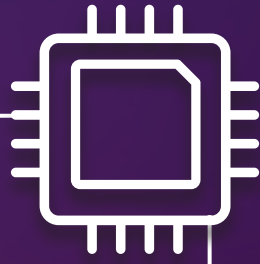
Client Communications

Family office service and estate planning is highly complex and personalized. One of the most important skills for a professional to possess is the ability to explain sophisticated concepts in a way that can be understood by the client, who may be unfamiliar with even general estate planning terminology. AI may be particularly useful with the translation of legalese into easily understood terms. A family office professional or an estate planning attorney may tell generative AI software to “Explain the generation-skipping tax exemption to a 10-year-old,” and the software will provide a simplified explanation of exactly that. Clients with little to no background in finance or estate planning may benefit from these AI-generated simplified outputs, whereas a more experienced client may be able to process higher-level concepts.

Potential Risks

Generative AI software is a work-in-progress, and there are a variety of concerns that family office professionals and estate planning attorneys should be aware of before using AI tools. Specifically, confidentiality and security are of utmost importance to clients. For generative AI to work, the software must be able to review existing documents, many of which may contain sensitive and confidential information. Clients may have concerns about where their confidential information is going and how it is being used. Professionals must be able to give accurate, satisfying answers to these questions, and be prepared to postpone or forego AI use if the client feels uncomfortable.

Within the estate planning and family office industries, generative AI tools may be able to simplify time-intensive processes, but the human relationships and personalized conversations in the family office and estate planning contexts of estate planning are crucial to client satisfaction. AI cannot comfort a grieving widow, play referee to a dispute between estranged siblings, or implement a family business succession plan. Only trusted confidants who have earned the confidence and trust of clients can implement a well-crafted — even AI-generated — plan into a long-term, sustainable solution. While clients may not hire estate attorneys specifically for these interpersonal services, such services are necessary for any meaningful client representation.



Sports AI

SPORTS

How AI is Changing the Sports Industry

[Richard Brand](#), [Eric Fishman](#), [Wesley T. Gee](#), [Anjelica L. Fuccillo](#), [Emily P. Caylor](#)

Much has changed since the “Moneyball” theory revolutionized how technology is used throughout the sports industry and influenced the way fans and experts consume and analyze sports. As is the case in other industries, the next generation of technology, artificial intelligence (AI), is beginning to be embraced by those within the sports world. While AI continues to evolve and gain more attention in everyday life, the sports industry is already seeing a rapid and impactful increase of AI presence and utility. Although AI has clear benefits, it also brings many legal implications. This alert examines the many ways in which AI is currently being used in the sports industry, some of the potential uses in the near future, and several key legal and practical considerations that should be considered as AI continues to be more broadly implemented.

Sports Betting and Fantasy Sports Contests

Sports betting has become a multibillion-dollar industry now that sports fans in many states may easily (and legally) place a bet or wager. With the increased usage — and the potential for financial gain — gamblers are turning to AI to gain an advantage. AI’s tools can assist users in streamlining data and comparing players, assessing the impact of an injury, and evaluating starting lineups and potential trades.

However, the reliance on AI as a decision-making mechanism has its risks, especially a financial risk to the user. Reliability of results, patterns, and predictions depends on accurate and up-to-date data inputs that are not accessible to the user. Therefore, it is important to disclose that AI tools do not guarantee success. This may be achieved by addressing the risks of using AI in Terms of Use (such as accuracy disclaimers) or emphasizing on operators’ websites that AI tools are for decision-making support (and not exclusively for decision-making).

Coaches’ and Front Office Personnel’s Preparation

Coaches and front office personnel are leveraging the tools afforded by AI to gain a competitive edge. The improved data processing capabilities can help coaches better evaluate player performance, identify areas that need improvement, and recognize the strengths and weaknesses of individual athletes. AI can also streamline film study by isolating the most relevant footage and recognizing patterns that may not be easily detectable to the human eye. Virtual reality, powered by AI, can immerse athletes in simulated environments to replicate opponents and help hone their skills. Moreover, AI’s algorithms and pattern recognition capabilities can potentially revolutionize player scouting and recruitment because they can forecast the skill level and success of prospects.

However, these tools rely heavily on data consumption, a complex legal issue that raises important questions on how data is gathered and stored. This type of AI technology also could create critical privacy, security, confidentiality, and content concerns.

Automated Officiating

An important benefit of AI is the elimination of human error and bias — two factors that tend to be at the center of attention when it comes to officiating sporting events. Professional sports leagues have already implemented automated technology in their officiating programs in an effort to make the inherently unreliable task of officiating more reliable. One example is Major League Baseball’s (MLB) testing of its AI-generated automated ball-strike (ABS) system to standardize umpires’ calling of balls and strikes. The ABS system was originally introduced on a limited basis in Minor League Baseball in 2022 to determine challenged ball/strike calls only. But for the 2023 Triple-A season, the ABS system has been more prominently incorporated: ball/strike calls for one-half of the season’s games are exclusively determined by the ABS system, while ball/strike calls for the other half of games are officiated by human umpires, with the ABS system deciding challenges only.

MLB’s embrace of the ABS system suggests that important stakeholders are beginning to realize that the benefits of automated officiating cannot be ignored. However, the reliability and accuracy remain at the forefront of discussion. As of the date of this guide, MLB has not announced that the ABS system will be used at the Major League level.

Athlete’s Health

AI’s learning capabilities have the potential to transform the medical field and reshape the way an athlete’s performance and health are evaluated. Wearable technology, which has been used to measure training performance across many leagues and levels for several years, provides live updates of athletes’ vitals and exertion levels. The data collected serves as a detection mechanism to assess whether an athlete is injury-prone, as well as a tool to create specialized training, rehabilitation, and nutrition programs to mitigate an athlete’s risk of injury (or further injury) and to optimize performance.

AI can also be a useful tool in promoting safer sports across all leagues as its capabilities have the ability to analyze and predict how, when, and where injuries occur, evaluate the degree of such injuries, and model the potential short and long-term effect of such injuries. This data can then be used to create safer equipment, support rule changes, and assist game preparation strategy (for example, limiting the amount of practice time to avoid overexertion).

Although there are clear benefits, the use of AI to protect and preserve an athlete’s health can trigger legal implications, particularly when personal information is collected and disclosed to third parties. AI users may be able to mitigate these legal risks by disclosing to athletes the nature of the data being collected and how it will be used and protected, as well as obtaining the appropriate consents to collect and disclose personal information.

Fan Engagement

Fan engagement is yet another area in which AI can be useful. Marketers can use AI as a tool to create a more interactive fan experience by creating personalized content, products, and services that bring fans closer to the game. AI platforms, such as [MILLIONS.co](#), tailor AI systems to sports marketers specifically by generating marketing campaigns with text-based inputs. Other AI platforms, such as [NTT Data](#), are being used to provide fans insight on plays in real time, event history, player information and statistics, and information about the venue.

In addition to the many uses of AI in-venue, AI can also change the way we consume sports broadcasts by utilizing [virtual venues](#) and interactive content. In doing so, AI removes geographic barriers to attending live events while creating a more immersive and interactive experience as compared to traditional two-dimensional broadcasts. Additionally, this year, both the [Masters](#) and [Wimbledon](#) partnered with IBM to provide AI commentary, which used language models trained in golf and tennis to produce spoken commentary alongside video clips on their websites.

While AI has the potential to elevate the fan experience, its use must be navigated carefully, especially with respect to surrounding content. Content produced without significant human control and involvement is not protectable by US copyright or patent laws, creating a class of works with no human author and potentially no usage restrictions. Generative

AI tools may also create works that could infringe the copyrights of existing works, trademarks, and likeness if used for commercial purposes without appropriate rights or permissions. The failure of AI users to implement procedures to evaluate any content produced by generative AI before using it for commercial purposes may expose themselves to potential intellectual property issues.

Security at Stadiums

Another way in which AI is changing the landscape of sports is the use of AI-powered facial recognition and other monitoring technology to make sporting events safer by detecting potential threats to safety. The tools provided by this technology create a more efficient (and hassle-free) security process for venue owners and operators, as it eliminates the time it takes to check bags or perform full-body pat downs of fans, personnel, and other guests entering the venue. Such tools also make for a more enjoyable experience for the fans, as they allow for quicker and less intrusive entry into venue.

While biometric data can be useful to make venues safer and operations more efficient, privacy issues and the potential for the perception of data misuse are major concerns. Venue operators can reduce the risk associated with the collection and storage by implementing policies that protect fans' privacy as much as possible and by establishing practices to ensure that these tools comply with internal data security and confidentiality standards. Similar to any third-party software, the security and data processing practices for these tools vary.

Key Takeaways

AI has the potential to fundamentally change the sports industry, from how sports are played to how fans consume sports content. Although adoption of AI in sports has already begun, the technology is still very much in its infancy, and it is not clear how it will continue to evolve and be further integrated into sports. As the industry continues to adopt this next-generation technology, stakeholders will need to closely examine the unique legal and regulatory implications inherent in the use of AI technology in sports.

ArentFox Schiff's Sports Practice group boasts one of the most experienced and diverse sports practices in the country and regularly advises sports organizations (including leagues, conferences, teams, and national governing bodies), players, sponsors, and investors on a broad variety of sports matters. As the industry moves forward with implementing AI, our skilled team of attorneys will assist clients in navigating the intricate regulatory environment of AI.

About Us



Your goals define our mission. Whether an immediate need or a long-term objective, ArentFox Schiff helps you reach your full potential. As industry insiders, we partner with you to develop practical business strategies and sophisticated legal solutions to achieve today's targets and anticipate tomorrow's problems. We get you across the finish line.