Benesch

AI REPORTER

A Publication of Benesch's AI Commission

The Year In AI: 2024 Roundup and Forward-Looking Guidance From the Benesch AI Commission

In This Issue

The Year In AI:
2024 Roundup and Forward-Looking Guidance From the Benesch AI Commission

Kris Chandler
Chair, AI Commission

It was a busy year for AI in 2024, and the Benesch AI Commission continued to follow the headlines and stay on top of legal developments. We wanted to take a look back at the year while also looking forward with some proactive guidance in this new year. In the pages that follow, you'll find a recap of headline-making AI news and developments in 2024, plus insights from our team as 2025 gets underway, including:

- Key considerations when it comes to crafting an AI governance policy best suited for your business
- What healthcare executives need to know about AI in the industry, including the legal risks involved and strategies to mitigate these challenges
- What to know about the world's first comprehensive legislation regulating AI, including the timeline for implementation of the EU AI Act and what businesses should start doing now to ensure compliance

We look forward to continuing to navigate this ever-evolving area of law with you. As always, we are here to answer any questions you may have, so please don't hesitate to reach out.

Steven M. Selna
Partner

2024 AI Headlines

In Big Tech, Amazon announced plans to invest $110 million in its Build on Trainium initiative to bolster academic AI research. The tech giant is also partnering with X-Energy and Energy Northwest, as well as investing $500 million to create and deploy a number of nuclear reactors to address the mounting energy needs of its AI initiative.

Elsewhere, Google, OpenAI and Microsoft formed the Coalition for Secure AI to create a framework for AI security. As more scrutiny falls on the AI sector, both in terms of regulation and litigation, it's not surprising that major players may look toward self-regulation.

In the courtroom, OpenAI continues to be assaulted by numerous lawsuits—the results of which will surely create a precedent for similar cases against other AI providers. To that end, the AI pioneer scored some minor victories as it secured partial dismissals in two copyright cases involving AI training.

OpenAI also secured a brief reprieve from Elon Musk's litigation antics after the billionaire dropped his lawsuit over the company's move toward a for-profit model. The victory was short-lived, however, as Musk not only refiled his lawsuit but also expanded it to include OpenAI's former partner, Microsoft.

Perhaps the biggest AI news of the year was the EU's passing of the world's first comprehensive AI law, which our team covers in-depth starting on page 15. The law bans AI applications that pose a risk to an individual's rights and imposes restrictions on high-risk applications. While lauded by some, the law still has several kinks to work out since its implementation in August.

Closer to home, a number of U.S. states have begun introducing and passing AI-related laws, with California leading the way. The federal government also introduced a pair of AI-related bills that are meant to protect artists from deepfakes and to promote AI innovation in the financial service sector.

These developments, plus more 2024 highlights, appear on the following pages.

Sydney E. Allen
Associate

AI in Business | 2024 Headlines

IMF says nearly 40% of global employment could be disrupted by AI

The International Monetary Fund (IMF) feels the issue could deepen inequality and is calling for governments to establish social safety nets and offer retraining programs to counter the impact of AI. The effects are expected to be felt more deeply in advanced economies than emerging markets, partly because white-collar workers are seen to be more at risk than manual laborers. In more developed economies, for example, as much as 60% of jobs could be impacted by AI. Approximately half of those may benefit from how AI promotes higher productivity, the IMF said.

Related: Generative artificial intelligence will lead to job cuts this year, CEOs say —Financial Times (sub. req.)

Source: CNN

OpenAI granted permission to train ChatGPT on Financial Times content

The Financial Times struck a deal in which it will receive an undisclosed payment in return for the ChatGPT maker using its content to train the AI. Users of the chatbot will receive summaries and quotes from FT journalism, as well as links to articles, in responses to prompts, where appropriate. This comes as the New York Times is suing the AI startup for allegedly using its content to train Large Language Models (LLMs) without consent.

Source: The Guardian

OpenAI allows creators to opt out of having their content train AI products

Following several lawsuits accusing the company of unlawfully using copyrighted content to train its AI models, OpenAI added privacy settings allowing regular users to remove their content so that it won't be used to train ChatGPT. The startup will thus deploy the Media Manager tool that lets creators opt out of training ChatGPT and other models that power OpenAI products.

Source: Microsoft Start

Sony Music Group opts out of AI training for signed artists

Sony Music Group (SMG) and its affiliates Sony Music Publishing and Sony Music Entertainment went on record, saying AI companies are not allowed to use the works of their recording artists for the purposes of training their systems. In its statement, SMG expressed its support for artists taking the lead in embracing new technologies but also highlighted the need to respect artists' rights, including copyrights. Popular artists and songwriters currently signed to SMG include Celine Dion, Doja Cat, Lil Nas X and 21 Savage, AC/DC,The Beatles, BTS, Bob Dylan and Amy Winehouse.

Source: Sony Music

Landmark Partnership brings News Corp content to OpenAI

Under a multi-year agreement, OpenAI has permission to display content from News Corp mastheads in response to user questions and to enhance its products in a push to bring reliable information to users. In addition to providing OpenAI with access to current and archived content from its major news and information publications, News Corp will share journalistic expertise. The partnership doesn't include access to content from any of News Corp's other businesses.

Source: OpenAI

continued on next page

Sydney E. Allen
Associate

AI in Business | 2024 Headlines

Google, OpenAI, Microsoft form coalition for secure AI

The Coalition for Secure AI (CoSAI), led by Google and including Microsoft and OpenAI, aims to create a framework for AI security, focusing on software supply chain security and mitigation strategies. Google's Secure AI Framework is the foundation for CoSAI's efforts, but challenges such as overlap with existing organizations and potential bias may affect its effectiveness.

Source: Android Police

Amazon investing $500M in nuclear power to meet AI energy needs

The retailer partnered with X-Energy and Energy Northwest to create and deploy a planned fleet of nuclear reactors with a total capacity of 5 gigawatts by 2040. Amazon said this is a response to the mounting energy needs of GenAI and its associated data centers. The planned build will initially see four advanced Small Modular Reactors in Washington state, providing up to 960 megawatts of energy—enough to power roughly 770,000 homes. AWS said it is also working with Dominion Energy to build a plant near the North Anna nuclear power station in Virginia.

Source: Maginative

Meta opens Llama AI to U.S. defense agencies, contractors

Meta Platforms approved the use of its AI models by U.S. government agencies and defense contractors, including Lockheed Martin, Booz Allen Hamilton Holding and Palantir Technologies. Meta's Llama is open source and available to over a dozen U.S. agencies and contractors. However, Meta's acceptable use policy restricts their use in certain projects.

Source: Bloomberg Law

Amazon invests $110M in academic GenAI research

The initiative, called Build on Trainium, will provide academic researchers access to a computer cluster with up to 40,000 Trainium chips, developed by Amazon Web Services for high-performance, low-cost deep learning. The investment is intended to address the resource bottleneck in AI academic research and support the development of novel GenAI applications.

Source: CIO Dive

Amazon launches AI chip, plans to rival Nvidia

Amazon is set to launch its Trainium 2 AI chip to reduce dependency on Nvidia and enhance operational efficiencies. The chip, designed for training large AI models, is already being tested by companies like Anthropic, Databricks and Deutsche Telekom. Additionally, Amazon's Inferentia chips are claimed to be 40% cheaper to run compared to Nvidia's alternatives for generating AI model responses.

Source: Techopedia

Carlo Lipson
Associate

AI Litigation & Regulation | 2024 Headlines

LITIGATION

OpenAI obtains partial dismissal of authors' copyright suit

A California federal judge rejected arguments by Sarah Silverman, Michael Chabon and other authors that the content generated by ChatGPT infringes their copyrights and that OpenAI unjustly enriched itself with their work. While other federal judges have also rejected claims that the output of generative AI systems violates the rights of copyright holders, they have yet to address the core question of whether tech companies' unauthorized use of material scraped from the internet to train AI infringes copyrights on a massive scale.

Source: Reuters (reg. req.)

Elon Musk drops lawsuit against OpenAI, founders

The suit was dropped just prior to a hearing during which the judge would consider defendants' motion to dismiss. The complaint alleged OpenAI and its co-founders, Sam Altman and Greg Brockman, breached their contract and fiduciary duty by allowing the company to become a for-profit entity that's largely under the control of Microsoft. According to Musk, the original intent behind the company was to develop general AI systems for the benefit of humanity. The move isn't surprising, given many experts believed the case was built on a very questionable legal foundation because the contract at the heart of the complaint wasn't a formal written agreement.

Source: CNBC

California court partially dismisses $1B copyright lawsuit against MS, OpenAI, GitHub

A California federal court dismissed in part a $1 billion class action lawsuit alleging Microsoft, OpenAI and GitHub used human-generated coding fragments without authorization to train the Copilot AI platform. The court held the developer plaintiffs failed to allege that their code was reproduced identically. The dismissal could have implications for transparency and data security in AI development by big tech companies.

Source: Law 360 (sub. req.)

California court partly dismisses OpenAI copyright class action

A California federal court dismissed unfair competition claims from a proposed class action against OpenAI filed by a group of authors, including Sarah Silverman, Junot Diaz and Andrew Sean Greer. The court ruled the claims under California's Unfair Competition Law (UCL) were preempted by the Copyright Act, which bars any state law claims involving rights within the general scope of copyright. According to the court, the UCL claims were based on the copying of plaintiffs' infringed works and would fall within the scope of the Copyright Act.

Source: Law 360 (sub. req.)

continued on next page

AI Litigation & Regulation | 2024 Headlines

California court denies in part motion to dismiss artists' copyright claims

A California federal court partly denied a motion to dismiss class action claims against Stability AI, Midjourney, DeviantArt and Runway AI, alleging the companies violated the rights of artists by scraping billions of copyrighted images without permission to train their AI systems. The court denied the motion regarding induced copyright infringement claims, holding plaintiffs plausibly alleged their works were used to train defendants' AI tools. However, the court dismissed Digital Millenium Copyright Act claims, breach of contract and breach of implied covenant of good faith claims.

Source: Law 360 (sub. req.)

California court dismisses OpenAI, Microsoft code copyright lawsuit

A California federal court dismissed a copyright lawsuit against OpenAI and Microsoft's GitHub, finding that plaintiffs failed to adequately allege that the Copilot tool could produce identical matches of copyrighted code. However, the court granted plaintiff's request for a mid-case appeal to the Ninth Circuit, which must determine whether OpenAI's copying of open-source code to train its AI model without proper attribution to the programmers could be a violation of the Digital Millennium Copyright Act.

Source: Bloomberg Law (sub. req.)

News outlets' lawsuit against OpenAI dismissed

A N.Y. federal court dismissed Raw Story and AlterNet's lawsuit against OpenAI, stating they failed to show actual injury from OpenAI's use of their copyrighted content to train ChatGPT. The court noted that the likelihood of ChatGPT outputting plagiarized content from the plaintiffs' articles is remote. However, the court acknowledged that legal questions remain about the use of copyrighted materials to train AI models.

Source: The Hill

Elon Musk expands OpenAI lawsuit to include Microsoft

The amended complaint, filed in federal court, accuses Microsoft of encouraging OpenAI's shift from a nonprofit to a for-profit entity. Musk claims this transition was part of a broader strategy by the tech giant to dominate the AI market and eliminate competitors, including Musk's own AI venture, xAI. The lawsuit alleges Microsoft's involvement facilitated anticompetitive practices, further strengthening OpenAI's market position.

Source: Law 360 (sub. req.)

X Corp. challenges California's deepfake law

The company argues A.B. 2655 is unconstitutional and violates Section 230 of the Communications Decency Act. According to X Corp., the law's enforcement system will lead to excessive censorship of political speech, limiting robust public debate. The law mandates large platforms remove or label deceptive deepfake content related to elections, excluding satire and parody. It also allows officials to seek injunctive relief for violations.

Source: Law 360 (sub. req.)

continued on next page

AI Litigation & Regulation | 2024 Headlines

REGULATION

China issues draft AI standardizing guidelines

The draft proposes to form more than 50 national and industry-wide standards for AI by 2026. China aimed to participate in forming more than 20 international standards for AI by that time. Of the prospective standards, 60% should aim to serve general key technologies and application development projects. This comes as the country attempts to catch up with the U.S. in AI development.

Source: Reuters (reg. req.)

EU approves world's first comprehensive AI law

The AI Act would ban AI applications that pose a clear risk to fundamental rights, such as those that involve the processing of biometric data. The law would also impose strict restrictions on " high-risk" systems, including those used in critical infrastructure, education, healthcare, law enforcement, border management, or elections. The Act also creates provisions addressing the risks of various AI systems, requiring producers to be transparent regarding the material used to train their models and to remain in compliance with EU copyright law.

Read more from our team: European Union Artificial Intelligence Act: An Overview

Source: BBC

Tenn. first state to adopt AI legislation protecting musicians

The Ensuring Likeness Voice and Image Security Act (ELVIS Act) expands upon the state's existing law that protect name, image and likeness by adding specific protections relating to generative AI. The bill creates penalties for individuals or organizations that use generative AI to produce an artist's name, photographs, voice or likeness without authorization. However, critics argue that the broad definitions included in the legislation could inadvertently limit certain performances, including when an actor is playing a well-known artist. Additionally, the law makes a person liable for civil action if an audio recording or a reproduction of a person's likeness was knowingly published without authorization, which has also raised concerns among critics.

Source: Law 360 (sub. req.)

Senate introduces legislation protecting artists from AI deepfakes

The NO FAKES Act would make individuals or companies liable for damages if they produce, host or share digital replicas of a person in audiovisual works, images or sound recordings without approval from the individual. The legislation responds to the increasing use of AI to create deepfakes, highlighting the need for laws to keep pace with advancing technology.

Source: Consequence

continued on next page

AI Litigation & Regulation | 2024 Headlines

Senate introduces bill to promote AI innovation in financial services sector

The Unleashing AI Innovation in Financial Services Act aims to foster collaboration between the private sector and government agencies to promote AI innovation that safeguards consumers in the financial services sector. The bill proposes the creation of controlled testing environments, or 'sandboxes', at financial regulators allowing them to experiment with AI technologies safely, encouraging innovation while ensuring consumer protection. The initiative is expected to strengthen the U.S. financial system and maintain the country's leading position in global financial technology.

Source: ExecutiveGov

U.S. forms $100M partnership with Big Tech to expand global AI use

The U.S. State Department will provide $100 million in funding and private sector commitments to expand global access to AI technologies. The initiative, in partnership with USAID, is part of the State Department's Partnership for Global Inclusivity on AI, aiming to make AI tools more accessible worldwide. Executives from OpenAI, NVIDIA, Amazon, Microsoft, IBM, Anthropic, Jacaranda Health, Google and Meta discussed their firms' initiatives to spread AI use globally. OpenAI introduced the OpenAI Academy to enable developers in developing nations to access the latest AI tools. The focus on inclusivity is seen as essential for addressing global challenges such as climate change, health crises and food insecurity.

Source: U.S. Department of State

California Governor vetoes landmark AI privacy bill

The proposed legislation sought to establish comprehensive guidelines for AI development and deployment, including transparency requirements and ethical standards. Gov. Newsom emphasized the need for a balanced approach that fosters technological advancement while addressing risks. He suggested federal regulation might be more appropriate given the global nature of AI technology.

Source: New York Times (sub. req.)

Meta opts out of EU AI Safety Pact to focus on compliance

Meta Platforms opted not to join the EU's voluntary AI safety pledge, which serves as a temporary measure before the AI Act takes effect in 2027. The company is prioritizing compliance with the upcoming AI Act, which will regulate AI development and require companies to disclose data used to train their models. The AI Pact aims to encourage companies to follow practices aligned with the AI Act's principles, such as assessing the risks of their AI tools in high-risk situations. The EU hopes to set standards for AI regulation without stifling innovation. Companies that sign the pledge may build trust with customers and regulators, while those that don't could face peer pressure and potential scrutiny.

Source: Bloomberg Law (sub. req.)

continued on next page

AI Litigation & Regulation | 2024 Headlines

N.Y. Dept. of Financial Services publishes AI cybersecurity guidelines

The guidance emphasizes the importance of robust governance frameworks, risk management practices and continuous monitoring to mitigate AI-related threats. It also highlights the need for transparency in AI systems, ensuring institutions can explain and justify AI-driven decisions. Additionally, the guidelines recommend regular audits and assessments to identify vulnerabilities and ensure compliance with regulatory standards.

Source: Law 360 (sub. req.)

Delaware, Georgia Supreme Courts regulate GenAI use

Delaware's interim policy, developed by the Delaware Commission on Law and Technology, allows judicial officers and court personnel to use approved GenAI tools, emphasizing user responsibility, informed use and compliance with laws. The policy prohibits the use of non-approved AI tools for non-public information and state resources. Meanwhile, Georgia's Supreme Court formed the Ad Hoc Committee on Artificial Intelligence and the Courts to assess AI's risks and benefits, aiming to protect public trust in the judicial system. The committee, comprising mostly judges and court administrators, will provide recommendations to ensure AI use doesn't undermine public confidence. Both states' actions reflect a growing need to balance technological advancements with ethical and legal standards in the judiciary.

Source: Law Sites

Benesch
AI ***Insights***

Kris Chandler
Chair, AI Commission

Alison K. Evans
Partner

Megan C. Parker
Associate

Key Considerations in Developing a Comprehensive AI Governance Policy and Mitigating Risks of AI Use

Crafting an AI Governance policy best suited for your business requires careful consideration of the types of AI, how AI will be used, current and future legislation, and a group of individuals specifically designated to oversee implementation of AI. Because of the significant developments in AI legislation in 2024 and the ongoing efforts to reform existing laws to adapt to AI development and deployment and the new legislative initiatives designed to address AI in 2025, it is becoming increasingly important for businesses to develop comprehensive and effective AI Governance policies that can accomplish legal compliance requirements and evolve within an increasingly volatile legal landscape.

With rapid advancements and new uses continuing in the realm of artificial intelligence (**AI**), all types of businesses are looking to find ways to utilize this technology as a powerful tool for increasing effectiveness and efficiency.

As a result, the need for comprehensive corporate policies governing the use of AI systems (**AI Governance policies**) within a business and mitigating risks associated with AI systems is becoming an increasingly important consideration for business leaders looking to stay ahead of the trend.

In crafting an AI Governance policy, each organization will need to balance the risks and benefits associated with use of AI in light of the specific challenges and opportunities it faces. Nonetheless, there are general considerations that every business should factor in when taking the next step toward AI Governance.

Defining AI and Uses are Important Starting Points

An AI Governance policy will need to take into account the different types of AI that a business may utilize. For example, an AI Governance policy covering use of a generative AI system should include provisions addressing human-involvement and supervision vs. a policy covering use of an algorithmic AI system.

Another important consideration in creating a comprehensive AI Governance policy is understanding the business's intended use cases. The level of scrutiny and oversight for AI systems that are used for internal purposes will be different than what is needed for customer-facing AI systems.

The type of AI systems and use cases will also vary depending on what industry a business is in, impacting what goes into a comprehensive AI Governance policy. For example, healthcare companies using AI to organize or analyze patient health information will need to consider including provisions based on HIPAA requirements, and financial institutions must be mindful of how their use of AI may impact their compliance with Gramm-Leach-Bliley obligations, whereas unregulated businesses may not be faced with such concerns.

continued on next page

Benesch AI Insights

Improve Upon Current Technology Governance Policies

While crafting new policies explicitly covering use of AI systems is important for any business as the technology continues to grow in importance, a business may be able to leverage current policies covering use of different technologies as a basis for how to govern its use of AI systems.

Revising and updating existing IT policies and procedures in a business to cover the AI lifecycle (e.g., development, deployment and ongoing monitoring of AI systems) can be an effective mechanism for developing early guidelines to implement AI systems within an organization.

Understand How Current and New Legislation Impacts AI

While most currently in force AI legislation focuses on consumer protection, businesses in highly regulated industries—such as healthcare, telecommunications and financial services, or those engaging in highly regulated activities—must evaluate how existing regulations may impact use of an AI system—even if the regulation is silent as to AI.

For example, a business that processes a significant amount of personal or sensitive data will need to ensure that its use of AI systems complies with applicable data protection regulations, such as the GDPR. This can include applying robust data security measures to an AI system using a recognized data security framework, obtaining proper consent before processing personal data in an AI training set, and using data anonymization or other privacy enhancing measures to protect personal data in AI models.

In addition to reviewing existing legislation and regulations, businesses should stay up to date on new legislation, case law and evolving industry standards to avoid falling behind or out of compliance. Joining working and industry groups, engaging with legal counsel and consultants, or even subscribing to newsletters with important AI updates can give businesses an edge in remaining compliant with AI regulations as they come into force.

Create an AI Governance Body Within the Business

While most corporate policies are reviewed on an annual basis, an AI Governance policy will require more oversight and adaptation because the technology is constantly changing. Businesses should designate a multi-disciplinary group of individuals from various departments within the organization to continuously review, update and implement an AI Governance policy. Many AI governance bodies are comprised of stakeholders from information technology, human resources and legal departments, to name a few.

The purpose of an AI Governance body should be to work toward collaboration and cooperation regarding use of AI systems, rather than just compliance, given the complexities this technology presents. Offering trainings to employees on proper uses of AI, documenting all uses to review efficiency and effectiveness, and providing guidance as the technology changes are all key roles necessary for an AI Governance body.

Consider Vendor Risk Management Issues

Not only should an AI Governance policy address a business's internal use of AI systems, but such a policy must also take into consideration how the business's third-party vendors are utilizing such tools. As more and more companies utilize AI systems to provide services, it is incumbent on businesses to have a plan for identifying those vendors that utilize AI systems in the provision of services, evaluating the security of those systems based on the applicable use case, and drafting appropriate contract terms.

Benesch's multidisciplinary AI Commission combines deep legal knowledge, technological know-how and incisive strategic business solutions. The team is prepared to assist our clients in crafting, implementing and overseeing a comprehensive AI Governance policy tailored to the specifics of the business, industry and use of AI.

Benesch
AI Insights

Navigating Legal Liability in AI Adoption: What Healthcare Executives Need to Know

Kathrin "Kat" Zaki
Associate

Nicholas "Nick" Adamson
Associate

The adoption of artificial intelligence (AI) in healthcare has ushered in a new era of innovation that is transforming diagnostics, treatment planning and operational efficiencies. However, with great potential comes significant legal and ethical responsibilities. For healthcare executives, understanding the unique inherent risks associated with AI adoption is critical to leveraging its benefits while avoiding potential liabilities.

Here's what you need to know about AI in healthcare, the legal risks involved and strategies to mitigate these challenges.

I. AI Uses in Healthcare, Legal Risks and Liability Issues

AI adoption in many industries is still in its infancy, however, implementation in healthcare has been swift. In general terms, usage of AI in healthcare can be divided into two broad categories: clinical implementations and non-clinical implementations. Some current clinical uses of AI in the marketplace include lab reading technologies, drug trial administration, creation of initial risk assessments and technologies assisting with developing patient-specific care plans. Current non-clinical AI uses in healthcare include predictive language clinical note taking, patient visit write-ups, billing and coding technologies, and patient research technologies.

All of these implementations of AI carry unique risk factors, but below are some broad liability concerns all providers should consider.

Malpractice and Regulatory Compliance

Malpractice liability relating to AI largely arises in the context of using clinical or diagnostic AI software. While it is likely that AI could bear some liability risk in the malpractice and clinical context, more of this risk will undoubtedly fall on providers. At the end of the day, licensed providers will be the ones responsible for their implementation and oversight of AI and will be the only party in privity of contract with patients who may experience ineffective treatment consequent to AI usage.

Administrative and Non-clinical Regulatory Risks

While non-clinical AI uses carry less risk from a patient care standpoint, such uses could still invoke regulatory scrutiny. For example, if multiple hospital systems in one small area use the same AI tool to generate off the rack pricing, the AI tool might inadvertently function to price fix the costs of services in that area which would violate antitrust laws. Antikickback concerns are also abundant here given that AI assisted billing and coding impacts what is submitted to federal and state payors, which can give rise to liability if the billing contains errors of any kind. As such, providers need to understand to what extent their contracted vendors are leveraging AI technologies in order to effectively contract around these risks.

Data Privacy and Vendor Accountability

Data usage is an especially high-risk aspect of AI technologies. As discussed below, AI trains itself using data inputs provided from its clients. As such, if multiple healthcare systems are using the same AI technology, there is a chance that the underlying data is being passed to other providers using that technology, even if the data isn't immediately apparent on a first glance. As such, it is important to hold AI vendors accountable for keeping data separate and not using it to train models used in other practices. It is also important to use bespoke contractual tools and language to address these unique privacy concerns to avoid inadvertent PHI or other business information disclosure.

continued on next page

II. Mitigating AI Risks: A Strategic Approach

Addressing the risks of AI in healthcare requires a strategic focus on data governance, compliance, oversight, education and vendor management.

Data Governance

Preventing bias through data governance is a critical first step. AI models must be trained on diverse and representative datasets to avoid reinforcing systemic inequalities. Organizations should regularly audit their AI tools to ensure they deliver equitable outcomes across all patient demographics. Establishing cross-functional AI committees can provide valuable oversight, helping to identify blind spots and address potential issues before they lead to harm.

Regulatory Compliance Framework

Compliance with regulatory requirements is another cornerstone of risk management. Organizations must navigate the complex landscape of federal and state laws governing AI use. Staying aligned with HIPAA regulations is essential, particularly in managing how protected health information (PHI) is processed or stored by AI tools. With new proposed state laws, such as those in Utah, Illinois and Colorado, requiring disclosure of AI use, healthcare executives must proactively adopt practices that promote transparency and secure proper consent.

By adopting well-recognized frameworks such as the NIST AI Risk Management Framework or ISO standards, organizations can promote responsible AI use. Governance policies should be clear and tailored to the needs of the organization, whether applied enterprise-wide or to specific departments. Senior leaders must play an active role in overseeing AI initiatives, ensuring that policies are implemented effectively and adjusted as technologies and regulations evolve.

Education and Training

Education and training are equally important in mitigating AI risks. Employees and stakeholders need a clear understanding of AI's capabilities, limitations and ethical considerations to adequately safeguard information funneled through AI systems. This requires ongoing education tailored to the roles and responsibilities of staff. Tools that pose higher risks (e.g. diagnostic AI tools, AI notetaking tools for patient intake, etc.) should be accompanied by specialized training to ensure that users can identify and mitigate potential issues in their workflows.

Vendor Quality and Management

Selecting and managing vendor relationships is another area that demands careful attention. AI tools often come from third-party vendors, and organizations must thoroughly assess these tools to ensure they meet industry standards of safety, validity and fairness. Ideally, vendors should possess appropriate security certifications, such as SOC 2 or ISO 27001, to ensure robust data protection. Contracts with vendors should include clear terms for data usage, compliance with laws and routine monitoring. To safeguard against potential failures, agreements should also include provisions for incident response and termination in the event of non-compliance or poor performance.

By integrating these strategies into their operations, healthcare organizations can mitigate the risks associated with AI, setting the stage for a more trustworthy and effective deployment of this transformative technology.

III. Top Takeaways for Healthcare Executives:

1. **Ensure Regulatory Compliance and Clinical Oversight:** Stay updated on HIPAA, FDA and emerging state laws, and form

continued on next page

cross-functional teams for oversight and accountability; in addition, ensure all clinical AI uses have provider oversight that is well documented.

2. **Demand Transparency from Vendors:** Be aware of what AI tools every vendor uses and require thorough documentation, indemnification and audit rights when negotiating vendor agreements. Ensure that BAAs and other privacy tools are tailored to the unique concerns of AI learning.
3. **Prepare for Incidents:** Regularly evaluate AI tools for performance and compliance, and develop a comprehensive process for addressing data breaches and model errors.
4. **Invest in Training:** Educate teams on safe and effective AI usage, including development of AI Use Policies and Procedures.
5. **Prioritize Patient Trust:** Be transparent about AI usage and its benefits for patient care, and ensure patients have the ability to opt in or out of AI use wherever possible.

Daniel S. Marks
Partner

Shivdutt Trivedi
Associate

European Union Artificial Intelligence Act: An Overview

World's first comprehensive regulation: The European Union Artificial Intelligence Act ("EU AI Act") entered into force on August 1, 2024.

Brief History

In October of 2020, the leaders of the European Union ("EU") requested the European Commission to propose ways to increase investments in AI systems and to provide an overarching regulatory framework for the same. The intention behind this request was that EU leaders wanted to strike a balance between fostering innovation and having AI systems that are transparent, safe and non-discriminatory. In response, a year later, the European Commission proposed an Artificial Intelligence Act on April 21, 2021. The European Parliament approved its version of the EU AI Act on June 14, 2023. This was followed by intense negotiations between the European Institutions (European Parliament, the European Council and the European Commission), and on December 8, 2023, the stakeholders reached a provisional agreement on the draft of the EU AI Act. Subsequently, on March 13, 2024, the EU AI Act received its final assent from the EU Parliament with 523 votes in favor, 46 against and 49 abstentions, bringing it one step closer to adoption. Thereafter, the final approved version was published in the Official Journal of the EU on July 12, 2024, and the EU AI Act came into effect on August 1, 2024. This is a historic moment, as the EU AI Act is the world's first comprehensive legislation regulating Artificial Intelligence ("AI") systems according to a risk-based approach.

Applicability

The EU AI Act will have broad applicability, much like the EU General Data Protection Regulation ("EU GDPR"), thereby having possible ramifications on companies established outside the EU. The EU AI Act applies to: (a) providers placing AI systems in the EU irrespective of where they are established; (b) deployers of AI systems that have their place of establishment in the EU; (c) providers or deployers located outside the EU but where the output produced by the AI system is going to be used in the EU; (d) importers and distributors of AI systems; (e) authorized representatives of providers of AI systems who are not established in the EU; and (f) affected persons that are located in the EU. One particularly important and intensely negotiated exception: the EU AI Act will not be applicable to AI systems that are used exclusively for military or

continued on next page

defense purposes.

Since the EU AI Act is going to apply to providers and deployers irrespective of the place of establishment, the implementation of this Act will have a ripple effect on companies established in the United States ("US") having operations in the European Union, even though the US has no overarching federal legislation at present governing AI systems akin to the EU AI Act.

Definition of AI Systems

In the absence of any other legislation, the EU AI Act will likely be the 'global standard' for regulating AI systems. To this effect, the definition of AI systems in the EU AI Act is in line with the Organization for Economic Co-operation and Development ("OECD") Guidelines. The EU AI Act defines AI systems as: "a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." This definition of AI systems is well thought-out to ensure that it is not only broad enough to envisage future technological advancements but also ensure that traditional software doing simple automated calculations are not included within the scope of this Act.

Risk-Based Approach

The EU AI Act will be modeled on a risk-based approach wherein high-risk AI systems will be regulated more extensively than the ones that pose less risk. To this effect, the EU AI Act has divided AI systems into four categories:

(a) Unacceptable Risk: These types of AI systems are deemed a clear threat to the safety and livelihood of humankind and go against the ethos of the EU. Therefore, such AI systems are prohibited by the EU AI Act. AI systems with unacceptable risk include (a) social scoring, (b) biometric identification systems used to deduce and categorize individuals on the basis of attributes such as race, sex life, sexual orientation and religious beliefs, (c) AI systems that manipulate human behavior. Even though these AI systems are prohibited, the EU AI Act carves out a narrow exception for such systems used for law enforcement purposes.

(b) High Risk: These types of AI systems are deemed to pose a significant threat to health, safety, fundamental rights and the rule of law. This type includes AI systems that are deployed in (a) critical infrastructure (e.g. transport, education, public utilities), (b) essential public services (e.g. credit scoring), (c) law enforcement that might impact a person's fundamental right; (d) administration of justice, (e) employment/recruitment, and (f) remote biometric identification systems. These AI systems will be required to comply with extensive obligations before they are available in the public market, such as, adequate risk assessment, appropriate human oversight and implementing mitigation systems.

(c) Limited Risk: These types of AI systems are deemed not to pose any serious threat and the primary risk associated with such AI systems is due to lack of transparency. The EU AI Act has introduced certain transparency obligations to ensure that all human users are well-informed that they are interacting with an AI system. An example of AI systems with limited risk is chatbots. As long as human users are made aware that they are interacting with a limited risk AI system, such system is not deemed to pose any significant threat under the EU AI Act.

(d) Minimal Risk: These types of AI systems are deemed to have no real associated risk and can be deployed without any restrictions.

continued on next page

Examples of minimal-risk AI systems include AI-enabled video games and inventory-management systems.

General Purpose AI (GPAI) Systems

As the name suggests, GPAI systems are those AI solutions that can be used for a variety of different purposes. The AI Act will not apply to GPAI systems that are used exclusively for the purpose of scientific research and development. However, GPAI systems used for other purposes will be regulated by the AI Act with a focus on maintaining transparency. For instance, the provider of a GPAI system will be required to make technical documentation available to the enforcement authorities for training and testing purposes. Further, the GPAI systems must be modeled in a way to respect the national copyright laws of the member states.

If a GPAI system's computational power is greater than 10^25 floating point operations (FLOPs), then such GPAI model is presumed to have high impact capabilities and will be subject to additional regulations. Further, the EU Commission intends to release a periodic list of such GPAI models with systemic risk to ensure compliance.

Fines

Much like the EU GDPR, the EU has proposed stringent fines to ensure compliance with the AI Act. The majority of the violations under the legislation will be subject to administrative fines of up to 15 million Euros or 3% of the violator's total worldwide turnover for the preceding financial year ("Total Turnover"), whichever is higher. However, violation of Article 5 (prohibited AI practices) will be subject to administrative fines of up to 35 million Euros or 7% of the violator's Total Turnover, whichever is higher. Further, the supply of incorrect, incomplete or misleading information to the notified bodies or national regulators in response to a request will be subject to administrative fines of up to 7.5 million Euros or 1% of the violator's Total Turnover, whichever is greater.

National Regulators

EU member states have been given until August 2, 2025, to nominate the relevant National Competent Authorities ("NCA") that will regulate the AI Act in each such member state. Each member state will be required to establish or designate three authorities at the national level: (1) Notifying Authority ("NA"): It will be tasked with setting up and carrying out procedures for assessing, designating and monitoring conformity assessment bodies; (2) Market Surveillance Authority ("MSA"): It will be tasked with taking measures to ensure that AI products comply with the legal requirements (NA and MSA will together be the NCA for respective member states); and (3) National Public Authorities ("NPA"): It will be tasked with enforcing fundamental rights obligations with respect to the High-risk AI Systems. The EU member states were required to nominate their respective NPAs by November 2, 2024.

The member states can use their own discretion in ascertaining the structure and design of these three authorities. For instance, Spain's Agency for the Supervision of Artificial Intelligence ("AESAI") is going to act as the country's single MSA. However, Finland is thinking of designating ten pre-existing market surveillance authorities as their MSA.

At this stage, it is premature to speculate who will be the final NCAs for respective member states. We will know about the final decision on NCAs only when they officially notify these appointments to the EU Commission. As of now, only Malta has officially designated both the MSA and NA.

Timeline for Implementation

Even though the EU AI Act came into force on August 1, 2024, its implementation will be phased

continued on next page

over time. The following are effective dates for certain key provisions of the EU AI Act:

(a) February 2, 2025: Prohibitions on AI systems with unacceptable risk.

(b) August 2, 2025: Provisions relating to NCA, GPAI models, Governance, Confidentiality and Penalties.

(c) August 2, 2026: The remainder of the EU AI Act except for provisions relating to AI systems with high-risk.

(d) August 2, 2027: Provisions relating to AI systems with high-risk.

Impact of the EU AI Act on Businesses

With the three-year phased implementation of the EU AI Act, businesses in the EU should start building a thorough roadmap to comply with all the obligations. Further, as discussed above, **the EU AI Act has extra-territorial applicability and therefore, even businesses outside of the EU should become cognizant of the required compliance obligations**. Generally, every business should first ascertain the AI systems it is currently using/developing or will likely be using in the near future. This list should be comprehensive and should cover AI systems used across departments. Once the repository is created, the next step is to classify each of the AI systems into four risk categories as set forth under the EU AI Act (and as discussed above). Such categorization will not only streamline the implementation process, but also make it easy for businesses to ascertain and comply with the numerous obligations under the EU AI Act. Lastly, to ensure timely implementation, businesses should consider (a) organizing internal trainings and awareness programs; and (b) establishing formal governance models that would oversee compliance with the EU AI Act.

Under the EU AI Act, all parties that are involved in the development, manufacturing, import, distribution or usage of AI systems will have certain obligations. However, the two main players to be regulated in the market would be 'providers' and 'deployers', both of which are defined under the EU AI Act. A 'provider' is a natural or a legal person that either develops an AI system or a GPAI, or places either of these into service under its own name or trademark, irrespective of whether it receives a payment for the same. In other words, a 'provider' could either be a developer or a business engaged that 'white label' AI systems. Since the EU AI Act has been modeled on a risk-based approach, providers of high-risk AI systems will have greater obligations. Some of the major obligations include (a) formulating written policies to ensure a thorough quality management system; (b) ensure it conducts a conformity assessment before the applicable AI system is placed on the market; (c) compulsory registration with the EU and affix the 'CE' mark suggesting that the AI system meets the compliance requirements; (d) report major incidents including serious physical harm of person/property or violation of fundamental rights to the relevant MSA; and (e) comply with accessibility requirements. Therefore, providers under the EU AI Act will be held accountable for the overall safety of AI systems.

'Deployers' are defined as any entity that is using the AI system in a professional capacity under its authority. In other words, any business that uses an AI system in the US for either internal purposes or for providing services to its customers will fall within the definition of deployers. Additionally, as stated earlier, even if an AI system is not in the EU, but if the output generated by such AI system is going to be used in the EU, such deployers would also be required to comply with the applicable obligations. Therefore, majority of the businesses will fall under the category of 'deployers'.

continued on next page

Moreover, specifically for high-risk systems, a 'deployer' may also be considered as a 'provider' if (a) uses its mark on the high-risk AI systems; (b) makes major modifications to a high-risk AI system; or (c) substantially modifies an AI system that it subsequently becomes a high-risk AI system. In either of the above scenarios, the deployer will now have to also adhere to all the obligations applicable to a 'provider' under the EU AI Act.

With respect to all AI systems, irrespective of the risk associated with it, deployers are obligated to ensure a suitable level of AI literacy of their staff or any other stakeholder using the AI system. Deployers also have a duty to cooperate with the NCA and NPA for any AI system that poses some risk. Further, deployers of specific AI systems have certain transparency obligations. For instance, deployers of emotion recognition or biometric categorization systems must notify the individuals that are subject to such AI systems and must process their personal data in accordance with the applicable data protection laws. Similarly, deployers of generative AI and deepfakes must disclose that the output is generated by an AI system.

Some of the major obligations for a deployer of a high-risk AI system includes: (a) using the AI systems in accordance with use instructions. Additionally, provider must continue monitoring the use and notify the provider of any discrepancy with the use instructions; (b) assign a natural person(s) to oversee the training and overall implementation of the AI system; (c) notify its employees that the AI system they are using is categorized as a high-risk AI system. Additionally, if a high-risk AI system is used for critical infrastructure, similar notice must also be given to the end-users; (d) before first using the high-risk AI system, it must conduct a fundamental rights impact assessment to assess the risks associated with it and formulate mitigation actions that will be taken by the provider; (e) reporting serious incidents to the MSA; and (f) cooperate with the NCA in implementing the EU AI Act.

While the EU AI Act imposes various obligations on deployers and providers of AI systems, a structured and timely approach can ensure compliance with this new legislation. By integrating these requirements systematically, providers and deployers can stay ahead of the curve and foster legally compliant AI development.

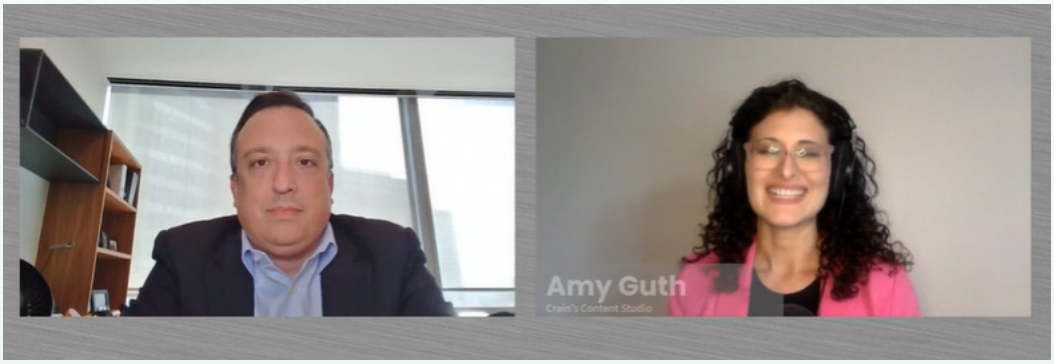
With the EU AI Act being effective and moving towards a phased implementation, and as other countries and US states begin to follow the EU's lead, the Benesch AI Commission remains your trusted partner for all things Artificial Intelligence and can assist your organization as you navigate these new rules and compliance obligations. For more information, please reach out to a member of the team.

2024 SPEAKING & EVENTS ROUNDUP

Our talented attorneys continued to be a part of the AI conversation in 2024, contributing their insights to several distinguished events and panels while exploring the latest AI developments and legal implications.

MAY

Ryan Sulkin spoke with *Crain's Chicago Business* host Amy Guth about what businesses should know when it comes to using AI responsibly. During the conversation, he discussed complexities in intellectual property, privacy compliance and risk management in AI adoption.



Kris Chandler participated in the CSU College of Law 2024 Cybersecurity & Privacy Protection Conference, speaking on the "AI Regulation and Assessment" panel. He discussed AI-related laws and their implications, the risks posed by AI systems and the challenges organizations face in developing AI governance.

continued on next page

Benesch

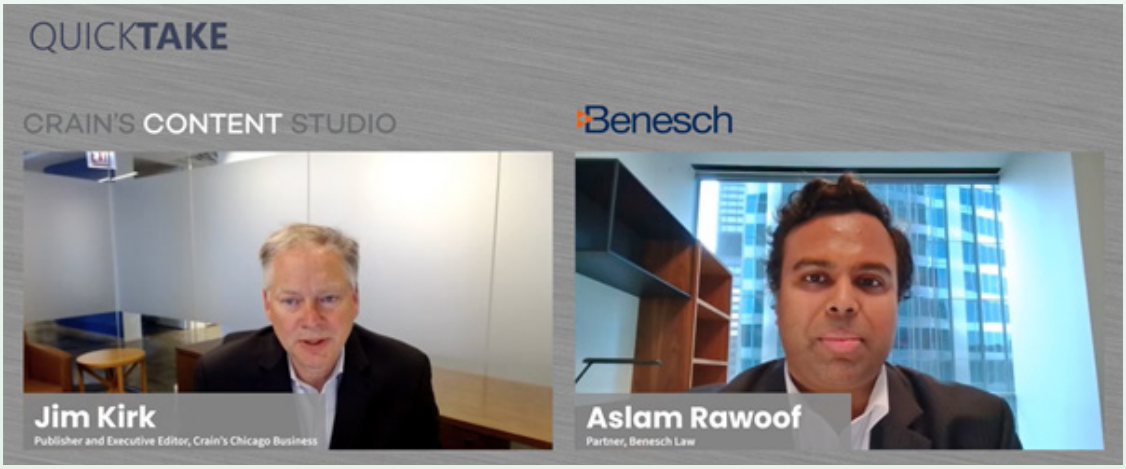
AI Insights

JUNE

Aslam Rawoof spoke at the AI Strategy Summit in New York. His panel, "Developing a Comprehensive Corporate AI Policy: Legal, Ethical and Compliance Considerations," covered how to balance innovation, IP protection and compliance when crafting AI policies.

SEPTEMBER

Aslam Rawoof discussed the critical need for establishing corporate policies on the use of AI in the workplace with Crain's Chicago Business publisher Jim Kirk. During the conversation, Aslam explored various considerations for business leaders, including securing organizational buy-in and adapting to the fast-paced advancements in AI technology.



OCTOBER

Benesch and Crain's Content Studio gathered a group of experts at the forefront of AI, including members of The Benesch AI Commission and two in-house counsel guests, for a panel entitled "Developing a Smart Corporate AI Policy." They provided guidance on steps every company should take to establish and maintain clear and relevant governance of AI in the workplace.

Shaneeda Jaffer participated in a panel at the Caribbean Regional Compliance Association Conference. Her panel, "TAKING AIM: AI and Compliance," explored the role of AI as it enables and disrupts the compliance space.

Benesch
AI Insights

NOVEMBER

Kris Chandler spoke on a panel at BVU's 2024 Civic Leadership Summit, covering the topic of AI as it pertains to nonprofits. The panel discussed practical, real-world applications to advance organizations' mission through increased efficiency and social impact.

Kris Chandler
Chair, AI Commission

UPCOMING SPEAKING ENGAGEMENTS

TIA 2025 Capital Ideas Conference

April 9–12, 2025
San Antonio, Texas

Kris Chandler will speak on the topic of AI at the upcoming TIA Capital Ideas Conference in San Antonio.

AMBA's 2025 Conference

May 7-9, 2025
Grand Rapids, Michigan

Kris Chandler will speak on the topic of Artificial Intelligence and Cybersecurity at the upcoming AMBA 2025 Conference in Grand Rapids.

Benesch AI Focus Area Leaders

Kristopher J. Chandler
AI Commission Chair
Data Privacy & Security

Ryan Sulkin
Contracting
Data Privacy & Cybersecurity

Alison Evans
Governance
Contracting

Daniel Marks
Intellectual Property (Ownership & Litigation)
Regulatory

Lidia Mowad
Intellectual Property (Ownership & Litigation)

Rick Hepp
Labor & Employment

Vince Nardone
Healthcare

Kelly Noll
Real Estate

Aslam Rawoof
Corporate

Katie Berens
Litigation

Juan Andres Mata
Litigation