Global AI trends report

Key legal issues for 2025

The legal issues in AI you need to know about for the year ahead

Introduction

Editors

Simon Elliott
Partner, Head of Data Privacy, Cybersecurity and AI for UK, Ireland and Middle East, London
D +44 20 7246 7423
simon.elliott@dentons.com

Giangiacomo Olivi
Partner, Europe Co-Head of Intellectual Property, Data and Technology, Milan
D +39 02 726 268 00
giangiacomo.olivi@dentons.com

As we enter 2025, we reflect on a period marking a paradigm shift in the adoption of artificial intelligence (AI). Major tech companies have poured more than US$150 billion into AI capital expenditure,[1] the overall AI market has pushed past US$184 billion[2] and there are reports acknowledging near 300 AI use cases across various industries.[3] Some organizations have evidently reaped these benefits, as valuations soar alongside the AI market's expansion.[4] 2024 unequivocally evidenced the ability of AI and its transformative potential to capture the focus of the market.

The market is already crystallizing into its next phase. Now, deployment of AI is no longer a concept or trial. It has the potential to contribute US$15.7 trillion to the global economy by 2030,[5] and major tech companies are already predicted to spend up to US$250 billion on AI infrastructure in 2025 alone.[6]

In the upcoming years, we expect to see business models increasingly shift to being AI-driven at the same time as new global regulations emerge, such as those developing more robust protections ensuring safe and responsible AI development. And there will be strong emphasis on business leaders having sufficient knowledge of AI to effectively navigate this shifting landscape.

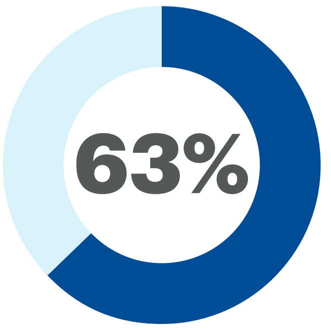
It is apparent that the green light is on for organizations to unlock AI's potential, and it is forming central pillars in business strategy and investment decisions around the globe.

However, it is imperative for businesses to be prepared before unlocking AI's potential. This involves staying informed about the developing issues and trends impacting the adoption of the technology, as well as preparing organizations' internal risk and operating structures.

Deployment of AI is no longer a concept or trial. It has the potential to contribute US$15.7 trillion to the global economy by 2030, and major tech companies are already predicted to spend up to US$250 billion on AI infrastructure in 2025 alone.

There will be strong emphasis on business leaders having sufficient knowledge of AI to effectively navigate this shifting landscape.

[1] https://www.forbes.com/sites/bethkindig/2024/11/14/ai-spending-to-exceed-a-quarter-trillion-next-year
[2] https://www.statista.com/forecasts/1474143/global-ai-market-size
[3] https://www.pwc.com/gx/en/issues/artificial-intelligence/publications/artificial-intelligence-study.htm
[4] https://www.reuters.com/technology/artificial-intelligence/openai-closes-66-billion-funding-haul-valuation-157-billion-with-investment-2024-10-02
[5] https://www.pwc.com/gx/en/issues/artificial-intelligence/publications/artificial-intelligence-study.html
[6] https://www.forbes.com/sites/bethkindig/2024/11/14/ai-spending-to-exceed-a-quarter-trillion-next-year



Notably, 63% of business leaders currently do not have a formalized AI roadmap.

Establishing robust building blocks from a governance perspective is essential to turbocharge AI strategy.

The approach to procurement or licensing of AI technology from external vendors is an area that is becoming increasingly "front of mind".

We recently surveyed 450 business leaders and general counsel to assess where large organizations are in their AI adoption journey and it was clear that, despite the AI hype, many are not at the stage of fully understanding where the technology can be transformative and executing on targeted strategic deployment.

For more detailed insights on how businesses are entering this new era of working with AI, please explore our Laws of AI Traction Report available at dentons.com.

Notably, 63% of business leaders currently do not have a formalized AI roadmap for high-impact AI integration. In a landscape where 74% of business leaders believe that AI is an important mechanism to protect their organization's revenue and bottom line, establishing robust building blocks from a governance perspective is essential to turbocharge AI strategy. While this varies by sector, the speed of AI adoption will depend on these building blocks to anticipate risks and help organizations close the gap between AI ambitions and the actions they take.

The growth of AI underscores the importance for businesses to readability position themselves to manage the associated risks of this evolving landscape. This report highlights what we at Dentons see as key legal and risk trends for AI in 2025.

For instance, AI's interaction with intellectual property rights is one of the most challenging issues needing near-term resolution and highlights emerging trends, such as growing attention on copyright concerns regarding potential infringement arising from the output from generative AI and what appropriate licensing partnership models should take. Considering this, organizations will need to consider safeguards and evaluate optimized protection strategies. This includes developing clear strategies on where licensing arrangements can protect or monetize content and looking to protect self-developed AI technologies by exploring specialist patent applications.

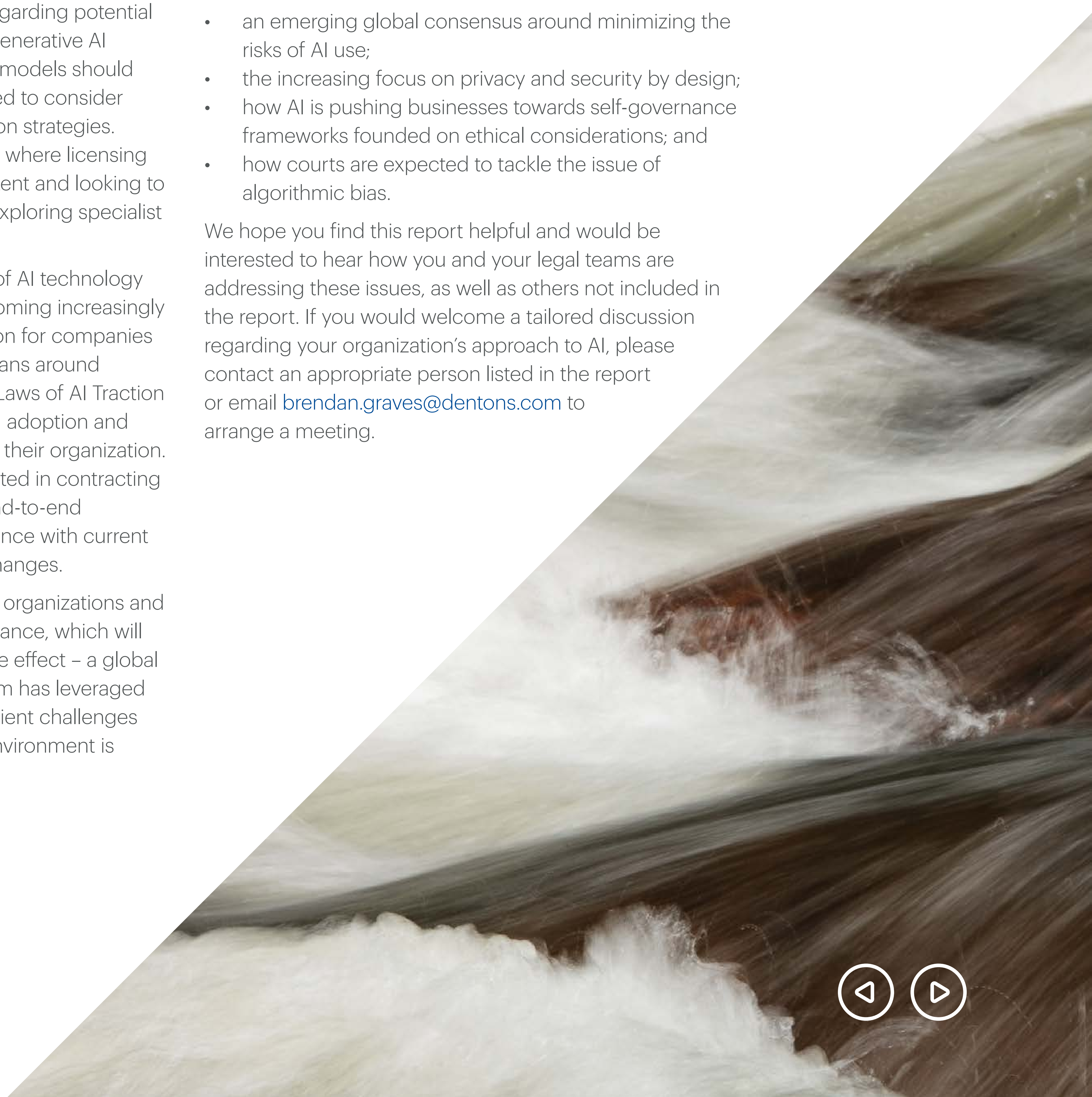
The approach to procurement or licensing of AI technology from external vendors is an area that is becoming increasingly "front of mind". This is a key strategic decision for companies focusing their growth and transformation plans around enhanced AI capabilities. According to our Laws of AI Traction Report, seven in 10 business leaders view AI adoption and implementation as the key growth driver for their organization. As this market evolves, organizations interested in contracting for external AI technology must consider end-to-end procurement strategies and ensure compliance with current AI regulations while anticipating potential changes.

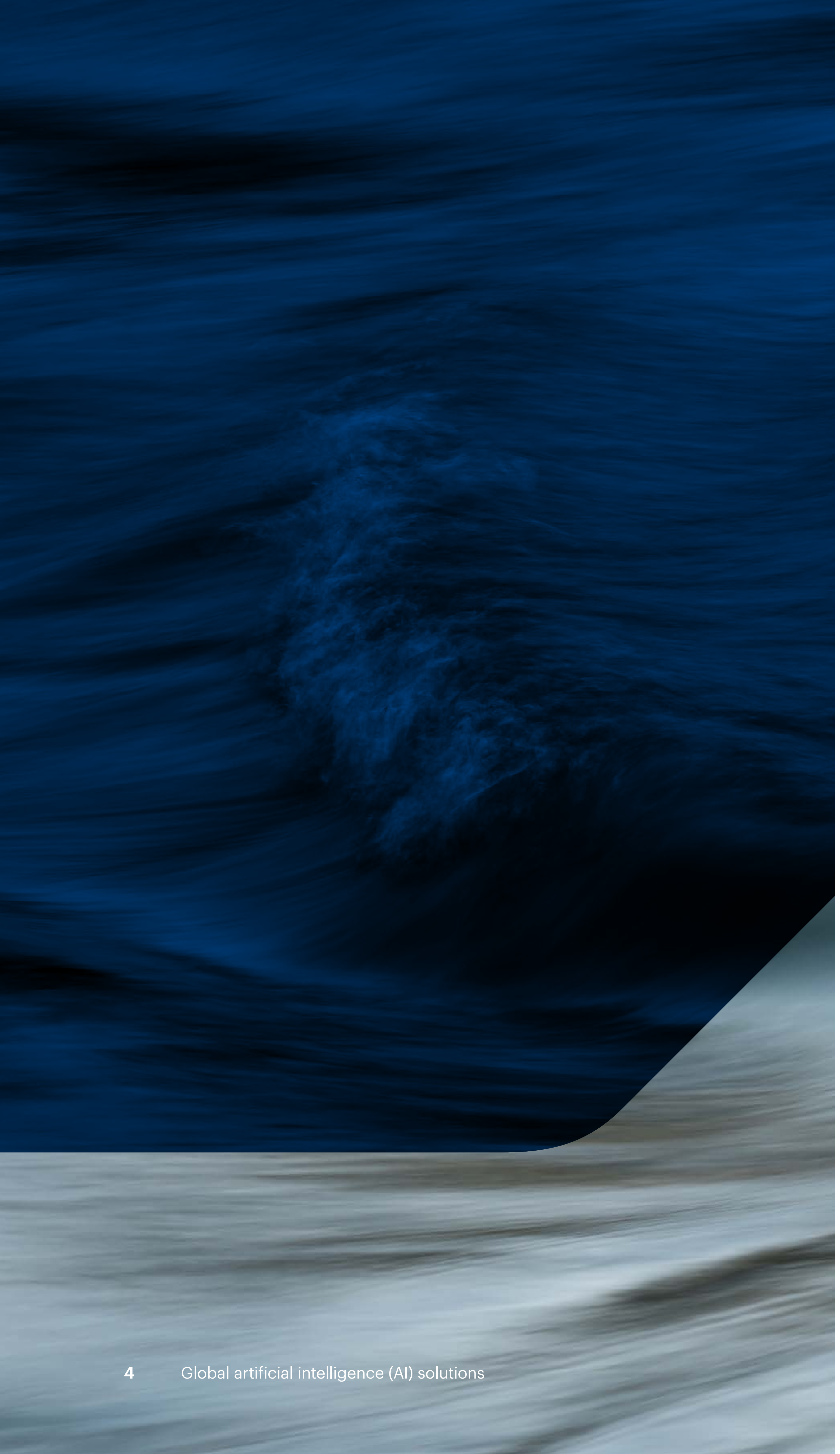
2025 is set to be another important year for organizations and leaders in terms of AI regulation and governance, which will see the initial provisions of the EU AI Act take effect – a global benchmark on AI regulation. Our global team has leveraged their understanding of current trends and client challenges to provide insights on how the regulatory environment is influencing approaches here.

Anyone with responsibility for their organization's legal or risk agenda will benefit from reviewing this report which also covers emerging issues such as:

- an emerging global consensus around minimizing the risks of AI use;
- the increasing focus on privacy and security by design;
- how AI is pushing businesses towards self-governance frameworks founded on ethical considerations; and
- how courts are expected to tackle the issue of algorithmic bias.

We hope you find this report helpful and would be interested to hear how you and your legal teams are addressing these issues, as well as others not included in the report. If you would welcome a tailored discussion regarding your organization's approach to AI, please contact an appropriate person listed in the report or email brendan.graves@dentons.com to arrange a meeting.





Contents

Regulatory cohesion starts to show the way forward

AI regulation, governance and ethics

Editor

Chantal Bernier
Of Counsel, Co-chair Global Privacy
& Cybersecurity Group, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

The global AI regulation landscape is fragmented and rapidly evolving. Earlier optimism that global policymakers would enhance cooperation and interoperability within the regulatory landscape now seems distant. Instead, we continue to see the policy process to regulate AI progress throughout the world at different stages and adopting different models, from policy statements to soft law, to tabled or adopted legislation.

However, through our support of global businesses, we see the beginnings of a common global direction emerging on how to minimize the risks of AI use and create the structures to address the core principles of safe and ethical AI development and use that are becoming the cornerstones of global AI regulations. In order to develop these AI governance structures, businesses need to anticipate evolving legal requirements and regulatory approaches.

Driven by this increasing cohesion, new governance models and strategies for AI have emerged in both the public and private sectors, offering valuable frameworks for other organizations to follow. For example, the European Commission's AI governance initiatives offer models from which companies can draw inspiration to avoid reinventing the wheel. Leading global technology companies increasingly provide a benchmark in their publicly available standards and principles. Globally, while there is a convergence around fundamental ethical principles and values, there remains a need to be cognizant of regional approaches to AI regulation and adopting organizations' own framework accordingly. Understanding these diverse strategies is crucial for companies operating in multiple jurisdictions.

In order to develop these AI governance structures, businesses need to anticipate evolving legal requirements and regulatory approaches.

Canada

Contributor

Chantal Bernier
Of Counsel, Co-chair Global Privacy
& Cybersecurity Group, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Canada's direction emerges from the proposed Artificial Intelligence and Data Act (AIDA) and the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems. With an election looming, AIDA has an uncertain future. The Voluntary Code commits the signatories to Accountability, Safety, Fairness and Equity, Transparency, Human Oversight and Monitoring, and Validity and Robustness.

United States

Contributors

Todd D. Daubert
Partner, Washington
D +1 202 408 6458
todd.daubert@dentons.com

Peter Z. Stockburger
Office Managing Partner, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com

The Trump administration likely will reduce regulation, minimize international cooperation and eliminate current Executive Orders with the goal of fostering innovation and US competitiveness. Plans may involve appointing an "AI czar" to coordinate federal efforts, focusing on infrastructure development like data centers and semiconductor manufacturing. This deregulatory approach may be resisted by skeptics, including key advisors. States will likely continue adopting sector-specific AI regulations to address concerns about safety and ethics, and courts will likely address key issues in pending cases. A fragmented and patchwork landscape will likely need to be navigated in the near-term.

Africa

Contributors

Shahid Sulaiman
Senior Partner, Cape Town
D +27 21 686 0740
shahid.sulaiman@dentons.com

Davin Olen
Associate, Johannesburg
D +27 11 326 6257
davin.olen@dentons.com

Efforts to regulate AI are emerging across Africa. Leaders across the continent include Mauritius, which has released an AI strategy, along with Kenya and Nigeria, which are both consulting with stakeholders to develop national AI strategies. In South Africa, stakeholder engagement has increased since the release of a draft AI policy framework for discussion. Further, South Africa's Patent Office has recently registered an AI as a patent inventor, contrasting with rejections of the same application elsewhere. This decision is based on the formative process for patent registrations in South Africa and provides an important incentive for AI development in the region.

Latin America

Contributor

Juanita Acosta
Partner, Bogota
D +57 601 743 9326
juanita.acosta@dentons.com

In Latin America, most countries only have soft law or equivalent instruments regarding the use of AI, except for Peru, which has implemented a regulation focused on principles and the promotion of AI usage.

Further details may be expected shortly, as several countries, such as Chile, Colombia, Brazil, Mexico, Panama, Peru and Costa Rica, are submitting bills and legal initiatives to regulate AI, particularly to protect personal data and intellectual property.

Latin America will continue to be a key region to watch in 2025.

United Kingdom

Contributor

Simon Elliott
Partner, Head of Data Privacy,
Cybersecurity and AI for UK,
Ireland and Middle East, London
D +44 20 7246 7423
simon.elliott@dentons.com

AI regulation in the United Kingdom finds itself in a challenging position.

Based on a clear vision in the UK National AI Strategy to continue as a global leader in supporting the development and adoption of AI (and aiming to unlock the economic benefits for in the digital economy and productivity), to date the UK has focused on a 'pro-innovation', light-touch approach centered on responsibility being placed on sectoral regulators to develop appropriate guidance and codes of practice and avoiding AI-specific legislation. "Guardrails" had previously been the watch word.

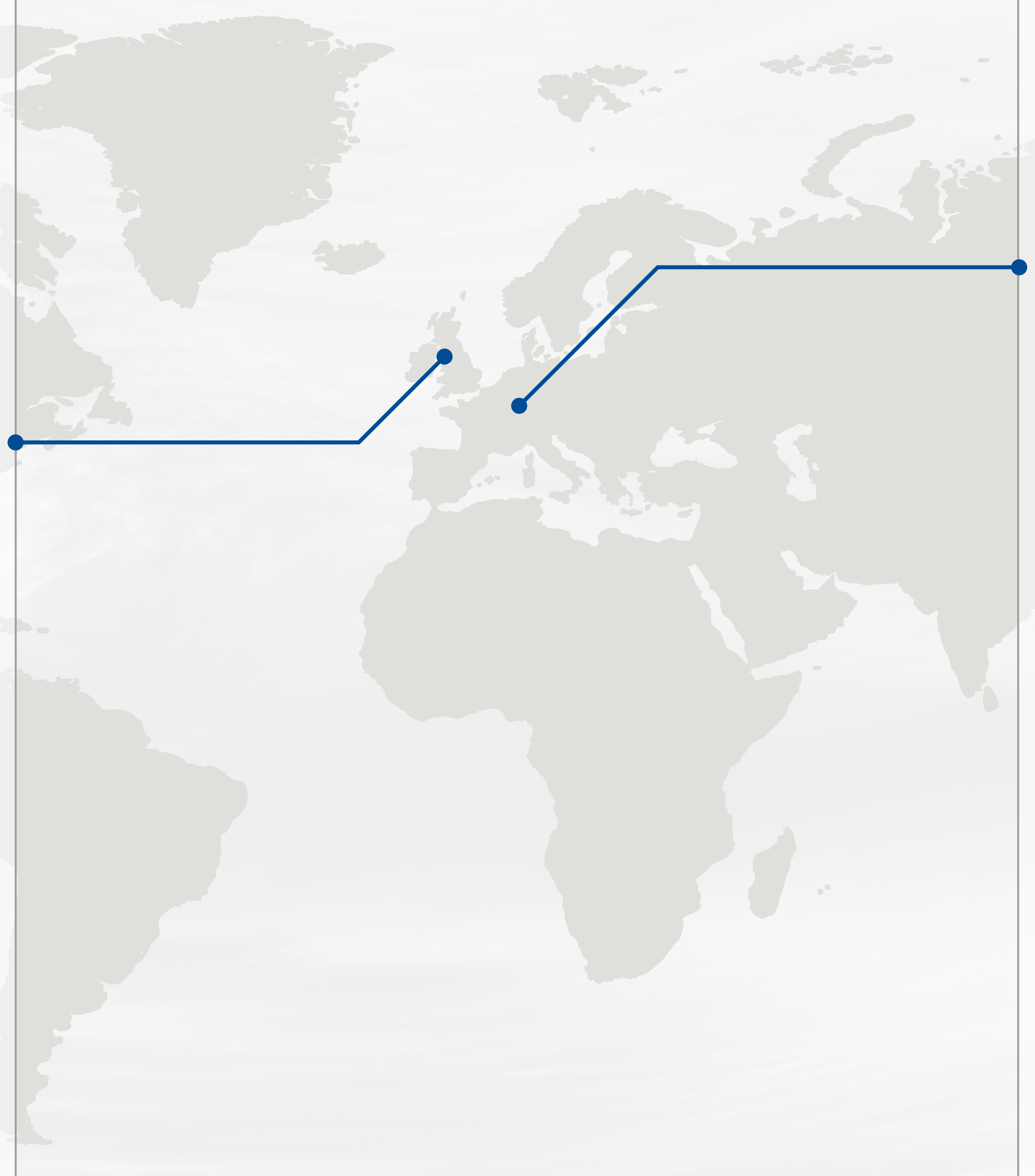
The UK has also seen its opportunity to be a balance or bridge between the safety-focused approach of the EU and the less regulated approach of the US.

However, there is a focus on the need to acknowledge an increasing consensus of the potential harms and risks that can arise from insufficiently regulated AI and to legislate accordingly.

The direction of travel appears to be an intention to do so, in a proportionate manner.

Details of a proposed legislative approach focusing specifically on the "most powerful" AI models are expected to be published for consultation shortly. Proposed legislation is likely to also involve codifying requirements for leading AI labs to make models available for testing.

This supports another key aspect of the UK's contribution to the global development and regulation of AI, positioning the UK AI Safety Institute as the global leader in undertaking and coordinating global research on the most important risks that AI presents to society to enable the best-informed policy decisions to be made. This will likely continue to be a key focus, particularly considering an anticipated scaling back of its US counterpart.



European Union

Contributors

Giangiacomo Olivi
Partner, Europe Co-Head of Intellectual
Property, Data and Technology, Milan
D +39 02 726 268 00
giangiacomo.olivi@dentons.com

Chiara Bocchi
Counsel, Milan
D +39 02 726 269 42
chiara.bocchi@dentons.com

Europe's regulatory strategy reflects its commitment to safeguarding fundamental rights, promoting trust in AI and shaping a global regulatory standard.

The European Union is indeed at the forefront of global efforts to regulate artificial intelligence, with its landmark AI Act.

The AI Act has been welcomed as the world's first comprehensive AI-specific legal framework, providing a legal definition of "AI System", and categorizing AI systems based on their potential risk for individuals and fundamental rights, focusing on the use of technology, rather than the technology per se.

Complementing the AI Act, the EU is advancing additional measures to address legal and liability challenges associated with AI. The proposed AI Liability Directive seeks to modernize non-contractual civil liability rules, ensuring they are equipped to handle the unique complexities of AI systems. Furthermore, the recent Revised Product Liability Directive extends liability to encompass software, AI systems and digital services that influence product performance – such as navigation tools in autonomous vehicles – bridging critical gaps in consumer protection.

Driven by this immediate and comprehensive legislation, new AI governance models are being deployed throughout the EU and will likely gain further traction from the newly established EU AI Office, fostering the promotion of the EU approach also beyond its borders. Many businesses – but not all - are turning to governance models designed for the EU AI Act as their benchmark model for managing compliance with developing global regulation.

Asia-Pacific

Contributors

Michael Park
Partner, Melbourne
D +61 3 9194 8313
michael.park@dentons.com

Matt Hennessy
Partner, Melbourne
D +61 3 9194 8389
matthew.hennessy@dentons.com

In September 2024, the Australian government released a Voluntary AI Safety Standard comprising a number of AI guardrails to create best practice guidance for the use of AI. The government also proposed mandatory guardrails for AI in high-risk settings, which were subject to public consultation. It is possible Australia could enact legislation drawing upon some of the concepts in the EU AI Act, but it currently remains unclear how the government will proceed. In May 2024, the Singapore government introduced the Model AI Governance Framework for Generative AI, which details best practice guidance on responsible development, deployment and use of AI. China's Interim Measures for the Management of Generative AI Services commenced in 2023 and should continue to be observed as the region's first comprehensive binding regulation on generative AI.

Privacy and security by design becoming the key cornerstones for effective AI risk management and digital resilience

Data privacy and cybersecurity

Editors

Todd D. Daubert
Partner, Washington
D +1 202 408 6458
todd.daubert@dentons.com

Peter Z. Stockburger
Office Managing Partner, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com

A convergence of rapidly evolving technological developments is leading to an increased focus on privacy and security by design and effective AI and data governance by companies and regulators around the world as the practical impact of AI on data privacy and security becomes clearer. The dynamic landscape of data privacy and security is demanding continuous adaptation from organizations and regulators, which privacy and security by design combined with strong governance help to achieve.

The past year was marked by an increased scrutiny of AI's impact on privacy, a heightened focus on protecting children's data, a need for businesses to adapt their models to comply with stricter data privacy laws and a growing practical risk arising from AI-enabled cyber threats.

Governments globally are enacting stricter data privacy regulations to protect personal information. Regulators are also scrutinizing the ethical implications of AI systems, prompting businesses to adopt privacy-preserving techniques like federated learning and differential privacy. Recent examples of AI-powered chat bots urging minors to engage in self-harm, suicide and violence against parents have led to intense scrutiny of whether these undesirable outcomes are the result of poor design choices or failures of governance.

The past year was marked by an increased scrutiny of AI's impact on privacy, a heightened focus on protecting children's data, a need for businesses to adapt their models to comply with stricter data privacy laws and a growing practical risk arising from AI-enabled cyber threats.

Engaging in privacy by design can help to reduce the likelihood that personal information used for training of AI models is disclosed in the results produced by the models or that personal data is incorporated into training data without appropriate consideration and mitigations.

As privacy laws become more complex and intertwined with AI-specific regulations, and as litigation risks increase, businesses face greater challenges in complying with inconsistent requirements without unnecessarily hindering technological innovation.

Privacy by design

Privacy by design – embedding privacy features into products, services and processes from their inception – has become a cornerstone for organizations prioritizing data protection, particularly in the AI age. By addressing privacy concerns early, businesses can ensure compliance, reduce risks and build consumer trust. Engaging in privacy by design can help to reduce the likelihood that personal information used for training of AI models is inappropriately disclosed in the results produced by the models or that personal data is incorporated into training data without appropriate consideration and mitigations. The widespread adoption of privacy by design signals a shift in attitudes toward privacy from treating privacy as a strategic asset rather than a mere afterthought. Companies embracing privacy by design are also better able to demonstrate a proactive commitment to transparency and responsibility, meeting the expectations of regulators and consumers for ethical data handling and AI development.

Cyberattacks

Cyberattacks, often supported by AI-powered tools, are more frequent and sophisticated, creating significant risks for organizations and governments worldwide. For example, Chinese state-linked hackers, known as "Salt Typhoon", infiltrated global telecommunications networks, compromising sensitive communications of senior officials. Integrating security by design is essential to withstanding these cyberattacks and enhancing digital resilience.

Many organizations are more effectively integrating security into the design of their systems, adopting zero trust architecture to more effectively control and verify access to resources, using AI to detect threats in real time, automate responses and prevent attacks, moving more data to the cloud to take advantage of third-party expertise, and implementing extended detection and response to integrate data from multiple security products into a single system to provide a more holistic view of potential threats. Robust and pragmatic governance structures and practices are critical for ensuring that the security measures implemented by design – security by design – continue to function as intended and remain updated with the latest intelligence and technology patches, and helping organizations that have suffered a security incident demonstrate that they had taken reasonable security measures to regulators and plaintiffs.

Collaboration among stakeholders is critical to address these challenges. Governments, industry groups and businesses are increasingly working more effectively together to establish global standards for data privacy and security, harmonize approaches and promote cross-border cooperation. Increased harmonization and collaboration would simplify compliance and enhance cybersecurity resilience.

In the face of rising cyber risks, stricter regulations and increasingly sophisticated technology, proper design and governance is a necessary foundation for balancing innovation with responsible risk management. Proactive, thoughtful and integrated approaches to data privacy and security will become increasingly important to efficiently navigate challenges and capture opportunities.

Cyberattacks, often supported by AI-powered tools, are more frequent and sophisticated, creating significant risks for organizations and governments worldwide.

The build vs buy dilemma continues

AI projects and procurement

Editor

Michael Park
Partner, Melbourne
D +61 3 9194 8313
michael.park@dentons.com

As organizations around the world continue to experiment with AI solutions and progress towards implementing AI systems as part of their internal business processes and products, many organizations are confronted with a stark choice: whether to "build" or "buy" an AI solution to meet their needs.

Unfortunately, there is no easy or "one-size-fits-all" answer to this question. On the one hand, many smaller or less technically sophisticated organizations lack the internal technical capability or resources to build or train their own AI solutions from scratch. Accordingly, these organizations are typically seeking to procure AI solutions from third-party providers. As part of these procurement activities, organizations need to grapple with new twists on a range of typical legal issues – including ownership of AI outputs, re-use of customers' inputs and data as training data for the supplier's other customers, and potential privacy and security concerns where personal information is used as an input – as well as novel legal issues, such as liability for so-called hallucinations in the output of AI models and other potential performance issues.

On the other hand, larger or technically sophisticated organizations may have the internal capability to build their own tailored AI solutions. In some cases, the "build" option may start with using a publicly available or open-source AI model that the organization deploys, refines and trains itself using its own proprietary datasets. Increasingly, the deployment of certain types of AI solutions can also require the use of specialized computing hardware to achieve the best possible performance. As a result, organizations that are seeking to build and train their own AI solutions are also having to consider whether to purchase and host the necessary computing hardware themselves or whether to obtain access to such hardware via third-party providers (in a manner similar to cloud computing). Consequently, most AI solution "builds" necessarily involve some element of "buy" as well.

For multinational organizations, the procurement and deployment of AI solutions on a global basis presents additional challenges. The governments of various countries around the world are taking differing approaches to the regulation of AI, ranging from a more prescriptive approach found in the European Union's AI Act to a more targeted or risk-based approach adopted by countries such as Australia. In light of this evolving regulatory landscape around the world, we are yet to see an emerging or settled consensus on what a "market" position is on various contractual terms for the supply of an AI solution. This could be impacting multinationals' "corporate agility" i.e. their ability to quickly adapt and respond to the opportunities offered by AI. Despite the challenges, we are seeing organizations endeavor to address the key contractual risks associated with AI-driven services in many template agreements.

We anticipate that organizations will continue to confront these issues throughout 2025 in this fast-moving space.

Build vs buy dilemma in the legal industry – key issues to consider

Editor

Břetislav Šimral
Europe Insight & Intelligence
Director, Prague
D +420 236 082 447
bretislav.simral@dentons.com

The debate around whether to build or buy generative AI solutions is also a pivotal consideration in the legal industry, where data confidentiality, workflow customization and cost-efficiency are critical. While in-house development offers long-term benefits in scalability, adaptability and control over sensitive processes, this approach is not without challenges, which can incentivize the outsourcing of the desired capabilities.

Size of firm

Smaller firms, for instance, may lack the technical expertise required to design and maintain such systems and the initial investment in infrastructure and talent can be prohibitively high. For these firms, partnering with external vendors to design and build tailored solutions can bridge the gap, allowing them to leverage expert capabilities without the full burden of internal development. Moreover, smaller teams might struggle to allocate resources for training and change management, which are critical for successful adoption throughout the firm.

Cost considerations

While third-party AI solutions provide a rapid entry point and occasionally even better out-of-box integration, they come with significant recurring costs that can easily accumulate into substantial annual operational expenses for large firms. By contrast, in-house development involves reasonable capital investment, and consumption-based operational costs, though these can be scaled predictably. Naturally, smaller firms may struggle with the initial investment and the resources needed to scale adoption effectively.

Data confidentiality

Many third-party tools operate in environments that may not meet the stringent privacy requirements of sensitive legal cases. In-house solutions provide greater control over data processing and ensure compliance with regulatory standards, protecting both client trust and organizational reputation. However, implementing secure, on-premises environments demands robust IT infrastructure, which smaller firms might lack.

Customization

Legal work often demands specific workflows that off-the-shelf tools cannot adequately address without costly modifications. Developing an internal solution allows organizations to tailor workflows and integrate complementary tools, ensuring the system evolves alongside their needs.

Scalability

Without the constraints of per-user licensing models, organizations can expand adoption across their workforce at minimal additional cost. This scalability is vital for embedding AI into daily workflows and maximizing its potential. Still, achieving widespread adoption requires investment in training and change management, which can be resource intensive. The rapid pace of technological advancement further supports the case for building.

Adaptability

Off-the-shelf solutions often lock firms into specific vendors, limiting flexibility as new capabilities emerge. An internally developed platform can integrate cutting-edge AI models and adapt to evolving needs, ensuring long-term relevance.

Building an in-house AI solution can enhance differentiation and strategic positioning. Proprietary platforms allow firms to stand out as leaders in legal innovation, attract top-tier talent and create new client-facing tools that drive revenue. Smaller firms can mitigate the challenges of building internally by forming partnerships with external vendors or adopting phased approaches that gradually integrate in-house capabilities. This strategy enables access to expertise while distributing the workload and investment over time, making the process more manageable. Nonetheless, smaller firms may find it challenging to capitalize on these opportunities without dedicated resources and clear strategic alignment.

While the benefits of in-house development are significant, this approach is not universally suitable. Smaller legal teams or firms without the necessary technical capabilities may find off-the-shelf solutions more practical in the short term. As tooling becomes more accessible and costs decline, building internally will likely become a viable option for a broader range of organizations. Advancements such as low-code and no-code platforms, pre-trained AI models and modular infrastructure components are increasingly reducing technical barriers, enabling even smaller firms to explore customized solutions with minimal development expertise. For firms with the capacity to invest strategically, prioritizing internal innovation can unlock the full potential of generative AI, delivering transformative value to clients and stakeholders.

Planning for workforce transformation

Employment and talent management

Editors

Purvis Ghani
Partner, Global Chair Employment and Labor Practice, London
D +44 20 7320 6133
purvis.ghani@dentons.com

Elouisa Crichton
Partner, Glasgow
D +44 141 271 5338
elouisa.crichton@dentons.com

Employment and people practices are a key component of any organization's AI roadmap, and this will continue to increase in 2025. The workplace of the future will need to have the skills and resources to effectively implement and leverage the benefits of AI and leaders need to consider how the technology may reshape their talent planning.

Companies will need to manage potential legal risks and must carefully consider employment law implications across different jurisdictions, including AI bias and discrimination in a range of areas, such as decision-making processes in recruitment and performance evaluations, and equality, diversity and inclusion impacts of use of AI in interactions with employees and customers. A few new and continuing key trends we anticipate for 2025, include:

AI decision-making

Companies will need to manage potential legal risks and must carefully consider employment law and data protection implications across different jurisdictions, including AI bias and discrimination in a range of areas, including decision-making processes in recruitment and performance evaluations, and equality, diversity and inclusion impacts of use of AI in interactions with employees and customers. Companies need to ensure that privacy notices are fit for purpose and future proofed to address any automated processing, that policies reflect the process for decision-making and that employers understand the need for human check and balance and ownership of decisions. This can also be relevant in contentious scenarios as it is key that people give evidence on decision-making.

The workplace of the future will need to have the skills and resources to effectively implement and leverage the benefits of AI and leaders need to consider how the technology may reshape their talent planning.

Companies will need to manage potential legal risks and must carefully consider employment law and data protection implications across different jurisdictions, including AI bias and discrimination in a range of areas.

Employees are using AI even where this is not led by the employer

Even where businesses do not have a proactive AI plan, staff are often experimenting with AI products themselves and engaging with them organically. There is a risk of inconsistent/inappropriate/unmonitored use of AI by staff. This could result in commercially or personally sensitive information being processed on AI software which is not controlled by or known by the employer. This risk can also arise in recruitment with candidates using AI during virtual interviews – employers should consider whether to permit this and design interviews with AI use in mind, or actively prohibit the use of AI and take steps to ensure it cannot be used to create an unfair advantage. Employers need to have updated policies and deliver training focusing on IT use/conduct/data protection policies and privacy notices to ensure appropriate limits, guidance and safeguards are in place.

Talent planning and skills gap risk

The prominence of AI means that different skills are valued and needed by many employers. Employees who can get the best out of AI are valuable and that may mean a change in recruitment, progression, development and training strategies at all levels. However, there is a growing risk that AI prominence results in employees missing out on core learning with a risk of a skills gap forming. Companies need to understand what skills are needed, appropriate use of AI and how to factor in this changing skills profile into performance management, recruitment and retention exercises.

Employers need to have updated policies and deliver training focusing on IT use/conduct/data protection policies and privacy notices to ensure appropriate limits, guidance and safeguards are in place.

Companies need to understand what skills are needed, appropriate use of AI and how to factor in this changing skills profile into performance management, recruitment and retention exercises.

Increasing regulatory scrutiny anticipated in 2025

IP protection and enforcement

Editor

Robyn Chatwood
Partner, Melbourne
D +61 3 9194 8330
robyn.chatwood@dentons.com

The rapid advancement of AI continues to raise complex questions about the applicability of intellectual property (IP) laws to AI and AI-generated works. The unprecedented pace of development of this technology is pushing enterprises towards self-governance frameworks founded on ethical considerations. IP remains one of the leading and most contentious issues in respect of AI governance.

In 2025 and beyond, we expect to see governments across the world grappling with balancing strategies aimed at encouraging the development of AI and innovation while, at the same time, attempting to modernize IP and AI legal frameworks to account for AI.

Rights in input data used to train AI models and infringement of IP

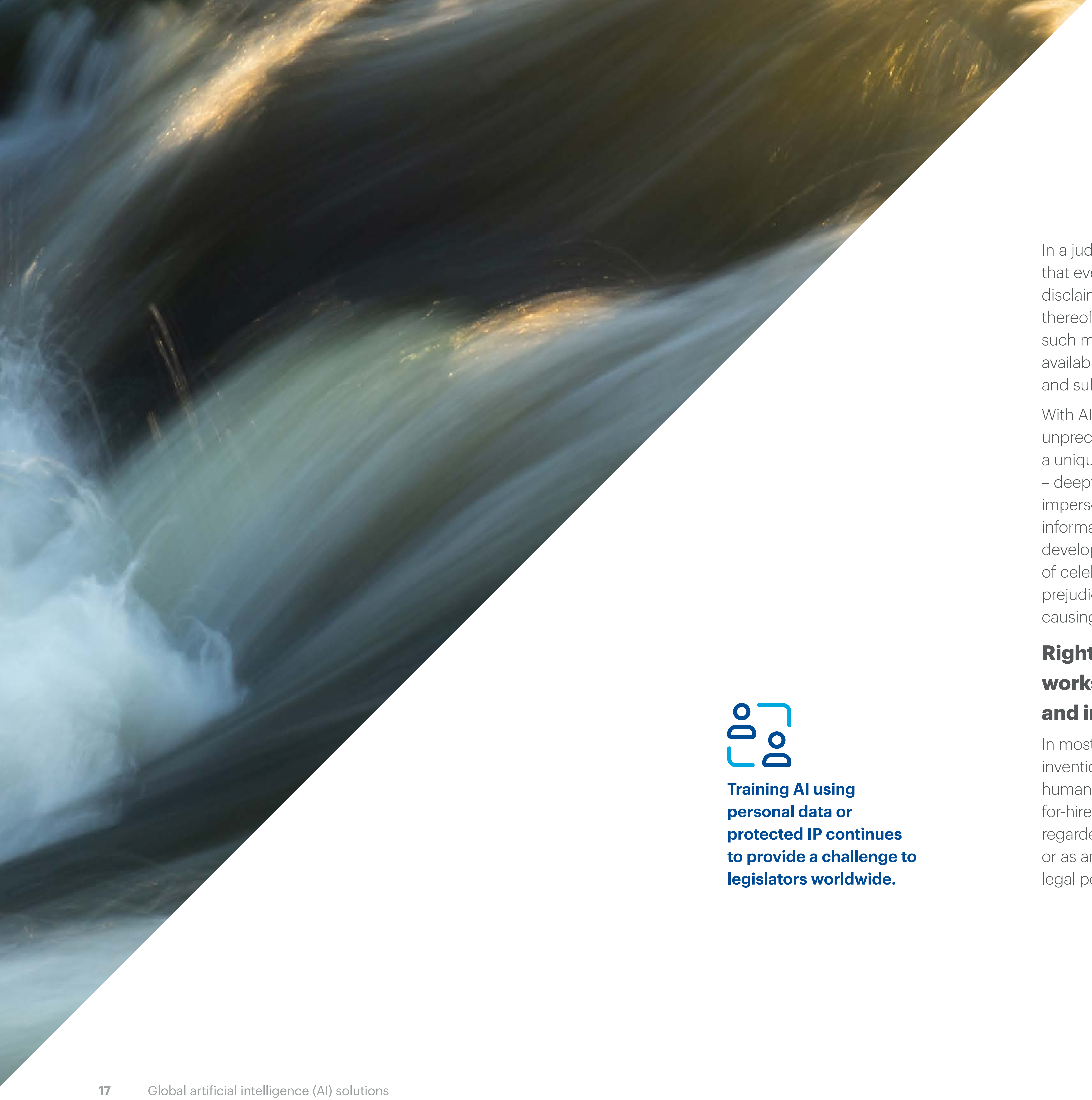
A highly debated topic is whether use of copyright-protected materials to train AI models should be considered as an infringement of the underlying copyright. Or should AI models be entitled to create new, derived content "informed" by the training data (as a real person may be having consumed the same source information)? This continues to provide a challenge to legislators worldwide.

In 2025, we expect to see increased regulatory scrutiny of organizations that create or use AI technologies which have been trained using information/data protected by IP rights. Regulators worldwide are now paying greater attention to balancing the benefits of AI against concerns about the protection of IP. By way of example, the Labour government elected in the UK in 2024 pledged to bring forward legislation tackling AI in 2025 and opened a consultation on the issue in December 2024. In the consultation, the government is seeking views on an extension of the express exception for text and data mining (TDM) to allow data mining for commercial purposes, coupled with the ability for rights holders to opt out, which would bring the UK more in line with the EU. The consultation runs until 25 February 2025.

The issue of IP infringement has taken center stage in global legislative discourse where AI models are trained on IP-protected data. While in some cases the right to scrape has been set out contractually between AI models and end-users, many large enterprises have been sued in various countries, in respect of unauthorized scraping of copyrighted work resulting in nuanced questions around fair use through democratized data mining of works in the public domain pending decision before the judiciary. Interestingly, many governments are leveraging AI to detect infringement and mitigate the risks.

The rapid advancement of AI continues to raise complex questions about the applicability of intellectual property (IP) laws to AI and AI-generated works.

We expect to see governments across the world grappling with balancing strategies aimed at encouraging the development of AI and innovation while, at the same time, attempting to modernize IP and AI legal frameworks to account for AI.



Training AI using personal data or protected IP continues to provide a challenge to legislators worldwide.

In a judgment of the Hamburg Regional Court, it was held that even a machine-understandable (vs machine-readable) disclaimer of a website specifically precluding the scraping thereof for the purpose of data mining would not preclude such mining done for scientific research that was publicly available without a cost. This decision is not res judicata yet and subject to debate.

With AI having the capability to generate images with unprecedented quality, it has also brought to the fore a unique issue within the larger ambit of infringement – deepfakes. Thus far, legislations have recognized impersonation as an offence under penal, privacy and information technology laws. However, in a landmark development, courts have recognized the personality of celebrities as being monetizable assets which are prejudiced by the emergence of deepfakes along with causing disrepute to their individual personas.

Rights in output data – AI-generated works, AI-inventions and other AI-outputs and infringement

In most countries, authorship of creative works and invention of new technology can only be attributed to humans and can be procured by corporations via a work-for-hire arrangement. A vital question is whether AI can be regarded as a legitimate author of the content it generates or as an inventor in the case of patents, given the lack of legal personality of the AI itself.

Pertinently, the Commission for Intellectual Property and Companies in Africa was the first global office to have granted a patent application where AI was the inventor. This move had received considerable backlash from other countries. However, the Hong Kong government has declared AI-generated works as being capable of copyright protection under the existing law. The US Patent Office has also issued a nuanced Inventorship Guidance providing a framework for examiners of patent applications to assess the quantum of human contribution for the invention to qualify for patent protection – a move seeking to balance IP rights with the need to leverage upcoming technology. In the UK as well, the law specifically permits copyright protection in "computer-generated works" though the broader question of originality being a precondition for IP protection continues to be ambiguous. In Europe, AI cannot be stated as inventor of a pate

Additional contributors include:

Joel Bock (US), Michael Franzinger (US), Sunita Kaur Chima (Malaysia), Jennifer Cass (UK), David Waggett (UK), Constantin Rehaag (Germany), Aliya Seitova (Kazakhstan), Jenni Rutter (New Zealand), Nadia Ormiston (New Zealand), Güneş Haksever (New Zealand), Davin Olen (South Africa), Shahid Sulaiman (South Africa), Catherine Lee (Singapore), Andre Rahadian (Indonesia), Minh Tran (Vietnam), Linh Tran (Vietnam), Richard Keady (Hong Kong), Julian Ng (Hong Kong) and Dong-Hwan Kim (South Korea).

The importance of proactive risk management

Disputes and managing liability

Editors

Peter Z. Stockburger
Office Managing Partner,
San Diego
D +1 619 595 8018
peter.stockburger@dentons.com

Craig Neilson
Partner, London
D +44 33 0222 1912
craig.neilson@dentons.com

Constantin Rehaag
Partner, Europe Co-Head of
Intellectual Property, Data and
Technology Group, Frankfurt
D +49 69 45 00 12 248
constantin.rehaag@dentons.com

Globally, dispute and litigation trends surrounding AI are evolving rapidly as the technology becomes more pervasive across industries. In 2025, we will continue to see courts grappling with the novel challenges AI presents, from defining liability for AI-driven decisions to addressing algorithmic bias that disproportionately affects protected classes.

National legislation applicable to the key areas we have outlined below has not been universally drafted to account for the challenges posed by AI and this factor, coupled with the rapid pace of technological advancement, ensures that AI-related disputes will remain a dynamic and contentious area of law. However, we have seen some dispute resolution bodies now offering bespoke rules for AI or other technology-related disputes to ensure that they are resolved as efficiently as possible with appropriate legal and technical expertise. 2024 saw key legislative initiatives, such as the EU AI Liability Directive. Businesses and policymakers alike will continue to be under growing pressure to anticipate and address these legal risks, emphasizing the need for robust governance, compliance frameworks and proactive risk management in the AI landscape.

We anticipate the following will remain a focus for disputes relating to AI in 2025:

Data and data privacy

A prominent area of concern is data privacy, where lawsuits are increasingly focusing on the unauthorized use of personal data to train AI models.

There are also growing concerns that the data utilized by AI systems is affected by unconscious bias in its processing or gathering. The litigation, regulatory and reputational risk may be particularly acute where the AI (whether or not with human oversight) is used to make decisions or recommendations impacting consumers. Employers should exercise particular caution in using AI to make decisions regarding their employees – various jurisdictions have seen litigation regarding discriminatory outcomes resulting from the use of AI in that context.

We will continue to see courts grappling with the novel challenges AI presents, from defining liability for AI-driven decisions to addressing algorithmic bias that disproportionately affects protected classes.

A prominent area of concern is data privacy, where lawsuits are increasingly focusing on the unauthorized use of personal data to train AI models.

Intellectual property

Various jurisdictions have seen a rise in intellectual property (IP) disputes as generative AI systems and their use of data challenge traditional notions of authorship and ownership under copyright law. Lawsuits continue to work their way through the courts over AI-generated content that allegedly incorporates copyrighted materials without proper licensing. The use of AI in this way is increasingly raising questions as to whether an AI model developer, trainer or user can be held liable where the AI makes use of IP-protected works in generating content. High-profile disputes, such as those involving news organizations and artists, are testing the limits of fair use and copyright infringement. This legal gray area is prompting calls for clearer legislative and judicial guidelines, at least in some jurisdictions. In Europe, many scholars and judges hold the opinion that the existing legal framework is sufficient to address copyright-related questions concerning AI, particularly regarding training, infringement and rights to the output. These topics have already attracted the attention of European law enforcement agencies.

Consumer protection

Consumer protection lawsuits are an emerging battleground. Claims often involve allegations of deceptive marketing of AI products or services, such as exaggerations about capabilities or failure to disclose risks. A false allegation that a company is using AI to improve its services can constitute a misleading commercial practice, for which the company making the false claim may be held liable.

Litigation around autonomous vehicles exemplifies these issues, with lawsuits targeting both the safety and transparency of AI systems in life-critical applications. Additionally, the US's Federal Trade Commission (FTC), for example, has warned companies against deploying AI tools that mislead consumers, further amplifying the potential for regulatory action. Initial decisions in Europe suggest that the user of an AI product may be primarily liable to their contractual partners, even if they did not develop the AI product themselves. As AI systems become embedded in more consumer-facing products, litigation related to product liability and algorithmic discrimination is expected to increase.

Cybersecurity

AI has significant potential to be used more widely to protect against the global threat of cyberattacks, by, for example, enhancing phishing protection and detecting insider threats. Equally, however, it also represents a threat, with new technology enabling new – and even more difficult to detect – threat vectors.

Standards of care owed by companies to their customers, suppliers and third parties are all likely to come under close scrutiny in this context as victims of fraud look to recover against identifiable and creditworthy parties who have unwittingly become involved on the peripheries of scams rather than fraudsters themselves, who may be difficult or impossible to trace and against whom enforcement may be impracticable.

As AI systems become embedded in more consumer-facing products, litigation related to product liability and algorithmic discrimination is expected to increase.

Advancing AI capabilities through M&A

M&A and investments

Editors

Arik Broadbent
Partner, Vancouver
D +1 604 648 6524
arik.broadbent@dentons.com

Constantin Rehaag
Partner, Europe Co-Head of Intellectual Property, Data and Technology Group, Frankfurt
D +49 69 45 00 12 248
constantin.rehaag@dentons.com

The surge in AI adoption has significantly influenced corporate strategies, including in the realm of mergers and acquisitions (M&A). The growing M&A activity is focused on companies acquiring related technology and technical talent to rapidly prepare for the disruption that AI is creating. Companies are increasingly leveraging M&A to enhance their AI capabilities, aiming to stay competitive in a rapidly evolving technological landscape.

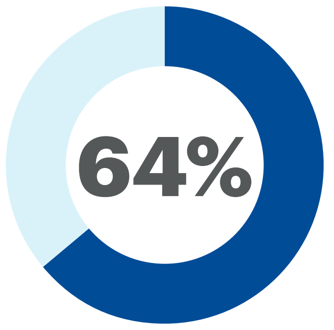
The role of AI in M&A

AI's integration into M&A transactions is multifaceted, encompassing the acquisition of AI technologies, skills and processes. According to our study, nearly two-thirds (64%) of business leaders plan to use M&A to bolster their AI capabilities within the next 12 months, with this figure rising to 70% over the next three years. Acquiring businesses with existing AI capabilities offers a relatively efficient way to onboard advanced technology and expertise, potentially leading to market expansion, enhanced agility and cost reductions.

However, the decision to pursue M&A for AI capabilities is not without challenges. The fast-paced and ever-changing AI landscape means there are significant gaps in the market and the uncertainty regarding which companies will ultimately rise to the top may compel organizations to consider alternative approaches. These alternatives include strategic partnerships with AI vendors and tech firms, taking minority stakes in AI organizations or purchasing third-party AI solutions as a service.

AI use also requires a number of inputs that are seeing dramatic increases in demand including increased computing power to run AI models. Major chip manufacturers have seen significant increases in demand for the components required to run AI models. AI also requires increased power, which is forcing governments and companies to consider how AI development growth can be supported by adding to existing power sources and energy grids, including renewed interest in nuclear power.

Companies are increasingly leveraging M&A to enhance their AI capabilities, aiming to stay competitive in a rapidly evolving technological landscape.



Nearly two-thirds (64%) of business leaders plan to use M&A to bolster their AI capabilities within the next 12 months.

Regulatory considerations: the EU AI Act

The regulatory environment surrounding AI is becoming increasingly stringent, particularly with the introduction of the EU Artificial Intelligence Act (AI Act). This legislation, which recently came into force, imposes comprehensive compliance requirements on providers, deployers, importers and distributors of AI systems. The AI Act categorizes AI systems based on their perceived risk, with certain high-risk AI systems subject to rigorous regulations, including human oversight, technical documentation and post-market monitoring.

In the context of M&A, identifying and categorizing AI systems and General-Purpose AI models within the target company is crucial. The AI Act's tiered approach to regulation means that AI systems employing manipulative techniques or exploiting vulnerabilities are entirely prohibited, with non-compliance resulting in substantial fines. High-risk AI systems, such as those used in employment or education, are subject to stringent rules, while other AI systems posing limited or no risks may fall outside the AI Act's scope.

Legal and compliance risks

Governments and regulatory organizations around the world have started developing legal principles and frameworks relating to the regulation of AI, with new regulations coming into effect on a regular basis. These regulations have the potential to impact AI transactions in two ways: (i) new opportunities to develop technology to adhere to the regulations, and (ii) new regulations that might negatively impact an AI company's service or strategy. Key themes of these regulations include human rights and equality, human oversight, transparency of AI use, sustainability and security.

The use of AI in M&A transactions also entails significant legal and compliance risks, particularly concerning copyright law. The ownership and licensing of the input, training data and output of AI systems are critical issues. The input and training data, which enable AI systems to learn and perform tasks, can be subject to copyright protection. The target company may have obtained these materials from various sources and, depending on the terms and conditions, may have limited rights to use, modify, share or transfer them.

The output of AI systems, which may be similar or identical to the input or training data, can also be protected by copyright or other statutory provisions. If the target company lacks the necessary rights or licenses to use, exploit, distribute or transfer the output, it may face liability risks, including claims for infringement, damages and injunctions. These risks could extend to the buyer, who may assume the target company's liabilities post-acquisition.

Due diligence and mitigation strategies

As executives and professional advisors improve their understanding of value generators and risks of AI-related companies, the due diligence process and purchase agreement negotiations are expanding to capture AI-related concepts of data use and ownership, copyright development and forthcoming regulatory risk. This underscores the importance for AI-related companies to evaluate their advisors' expertise in a rapidly developing specialized transactional marketplace. We also anticipate that there will be a significant increase in data owners enforcing their copyrights in data sets used without the owner's consent or a license to do so.

Private equity's increasing involvement in AI M&A

Over the past three years, it was estimated that 30% of AI-related M&A transactions were completed by a financial acquiror.[7] There are a number of factors that we see supporting this level of private equity (PE) involvement. Artificial intelligence is poised to impact many traditional industries where PE funds hold ownership positions. The transformational possibilities of AI adoption in those industries can create significant efficiencies in operations, and operational efficiency improvement is a fundamental lever for PE funds to deliver returns to investors, and which can also result in significant value creation for the AI companies in which these PE funds invest.

Although there are some indications that the available dry powder held by PE funds has decreased slightly in 2024, available cash for investments also remains at or near all-time historical highs.

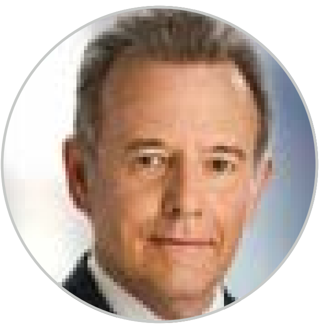
In conclusion, while M&A offers a strategic avenue for enhancing AI capabilities, it requires careful consideration of regulatory, legal and compliance risks. Companies must conduct comprehensive due diligence and consider alternative strategies to ensure a successful and compliant integration of AI technologies.

[7] https://aventis-advisors.com/ma-in-ai

“Killer collaborations” to algorithmic collusion

Competition and antitrust

Editor



Dr. Bertold Bär-Bouyssière
Partner, Brussels
D +32 2 552 2977
bertold.baer-bouyssiere@dentons.com

In 2025, several trends are anticipated in the realm of competition law enforcement as it relates to AI, including:

Continued scrutiny from global competition regulators and emergence of AI regulations

Aside from attempts to catch or call in “killer acquisitions”, regulators increasingly scrutinize “killer collaborations” between tech giants and start-ups with foundational AI (large language) models, suspecting a risk to block rivals from accessing new critical AI inputs (e.g. data, cloud infrastructure and GPUs) (“foreclosure”). Some regulators even try to assert jurisdiction over the hiring of “key personnel”.

After decades of politically neutral and methodologically consensual antitrust enforcement, regulators around the globe are increasingly subject to political pressure or beginning to deviate from orthodoxy to pursue industrial policy goals or protectionist objectives (e.g. “national champions”).

Resources for classic ex-post enforcement of abusive conduct being scarce, the EU has introduced a series of ex-ante regulations that include provisions on the competitive conduct of the companies in scope, in particular “gatekeepers” (DMA, DSA, AI Act, etc.). The designation of companies as gatekeepers and other regulatory threshold features is expected to trigger litigation.

Data-rich companies with dominant positions or significant market power that resort to conduct such as discriminatory self-preferencing or biased targeted pricing, or that breach privacy/data rules, may become subject to ex-post enforcement even beyond the scope of the ex-ante regulations mentioned above.

After decades of politically neutral and methodologically consensual antitrust enforcement, regulators around the globe are increasingly subject to political pressure or beginning to deviate from orthodoxy to pursue industrial policy goals or protectionist objectives.

Algorithmic collusion

Algorithmic collusion is a growing concern among regulators and lawmakers. Competition law historically distinguishes between unlawful collusion and lawful parallel conduct (bizarrely called "tacit collusion"). Adapting own prices to those of competitors based on independent intelligence is lawful, while a collusive understanding between competitors to align prices is unlawful. Algorithms that monitor and adjust prices push that distinction to its limits.

The US Preventing Algorithmic Collusion Act of 2024 aims to address gaps in existing laws by banning the use of algorithms trained on non-public competitor data, imposing disclosure and auditing requirements and establishing presumptions of illegal price-fixing in certain algorithmic contexts.

US and EU regulators are scrutinizing cases where competitors use shared algorithms to align prices. US lawsuits like those against RealPage and Yardi Systems involve allegations that algorithms were used to fix rental prices by analyzing and sharing non-public competitor data, with regulators claiming that algorithms enable or enforce a tacit agreement between competitors without explicit communication.

The DOJ has emphasized that even tacit agreements facilitated by algorithms, such as adhering to pricing recommendations based on competitors' shared data, can violate antitrust rules. Less radical EU guidelines stipulate that the shared use of algorithms relying on sensitive pricing information could be an "object" infringement and even algorithm providers could be held liable if their tools foreseeably facilitate collusion.

Companies using advanced AI systems should proactively prevent them from independently developing collusive behaviors, raising questions about liability in the absence of direct human contact. This has prompted calls for more proactive auditing and transparency measures to prevent inadvertent breaches ("looking under the hood").

Global AI team

Our full-service global AI team provides solutions to help you successfully implement AI technologies to support your organization's strategy, while navigating the complexity of existing and future regulations.

With 75+ partners and fee earners advising in 80+ jurisdictions worldwide, our global AI team provides market-leading legal advice around the world. Our team comprises leading AI experts advising across all key areas. Visit Dentons' AI: Global Solutions Hub for the latest legal insights, webinar recordings and regulatory overviews from around the world.

Juanita Acosta
Partner, Bogota
D +57 601 743 9326
juanita.acosta@dentons.com

Henrietta Baker
Partner, Dubai
D+971 4 402 0800
henrietta.baker@dentons.com

Dr. Bertold Bär-Bouyssière
Partner, Brussels
D +32 2 552 2977
bertold.baer-bouyssiere@dentons.com

Chantal Bernier
Of Counsel, Co-chair Global Privacy & Cybersecurity Group, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Chiara Bocchi
Counsel, Milan
D +39 02 726 269 42
chiara.bocchi@dentons.com

Global AI team

Arik Broadbent
Partner, Vancouver
D +1 604 648 6524
arik.broadbent@dentons.com

Robyn Chatwood
Partner, Melbourne
D +61 3 9194 8330
robyn.chatwood@dentons.com

Elouisa Crichton
Partner, Glasgow
D +44 141 271 5338
elouisa.crichton@dentons.com

Todd D. Daubert
Partner, Washington
D +1 202 408 6458
todd.daubert@dentons.com

Kagan Dora
Partner, Istanbul
D +90 212 329 30 35
dora@baseak.com

Simon Elliott
Partner, Head of Data Privacy, Cybersecurity and AI for UK, Ireland and Middle East, London
D +44 20 7246 7423
simon.elliott@dentons.com

Purvis Ghani
Partner, Global Chair Employment and Labor Practice, London
D +44 20 7320 6133
purvis.ghani@dentons.com

Nusrat Hassan
Managing Partner, Mumbai
D +91 22 6625 2222
nusrat.hassan@dentonslinklegal.com

Matt Hennessy
Partner, Melbourne
D +61 3 9194 8389
matthew.hennessy@dentons.com

Kuan Hon
Of Counsel, London
D +44 20 7320 3940
kuan.hon@dentons.com

Global AI team

Zdeněk Kučera
Partner, Prague
D +420 236 082 283
zdenek.kucera@dentons.com

Karol Laskowski
Partner, Europe Head of Technology, Media and Telecommunications, Warsaw
D +48 22 242 51 27
karol.laskowski@dentons.com

Gilbert Leong
Partner, Singapore
D +65 6885 3638
gilbert.leong@dentons.com

Hayley Miller
Partner, Auckland
D +64 9 915 3366
hayley.miller@dentons.com

Craig Neilson
Partner, London
D +44 33 0222 1912
craig.neilson@dentons.com

Davin Olen
Associate, Johannesburg
D +27 11 326 6257
davin.olen@dentons.com

Giangiacomo Olivi
Partner, Europe Co-Head of Intellectual Property, Data and Technology, Milan
D +39 02 726 268 00
giangiacomo.olivi@dentons.com

Michael Park
Partner, Melbourne
D +61 3 9194 8313
michael.park@dentons.com

Antonis Patrikios
Partner, Co-chair Global Privacy & Cybersecurity Group and Global TMT Sector Lead, London
D +44 20 7246 7798
antonis.patrikios@dentons.com

Constantin Rehaag
Partner, Europe Co-Head of Intellectual Property, Data and Technology Group, Frankfurt
D +49 69 45 00 12 248
constantin.rehaag@dentons.com

Global AI team

Břetislav Šimral
Europe Insight & Intelligence
Director, Prague
D +420 236 082 447
bretislav.simral@dentons.com

Ambuj Sonal
Partner, Mumbai
D +91 22 6625 2222
ambuj.sonal@dentonslinklegal.com

Peter Z. Stockburger
Office Managing Partner, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com

Shahid Sulaiman
Senior Partner, Cape Town
D +27 21 686 0740
shahid.sulaiman@dentons.com

Kirsten Thompson
Partner, Toronto
D +1 416 863 4362
kirsten.thompson@dentons.com

ABOUT DENTONS

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you.

www.dentons.com