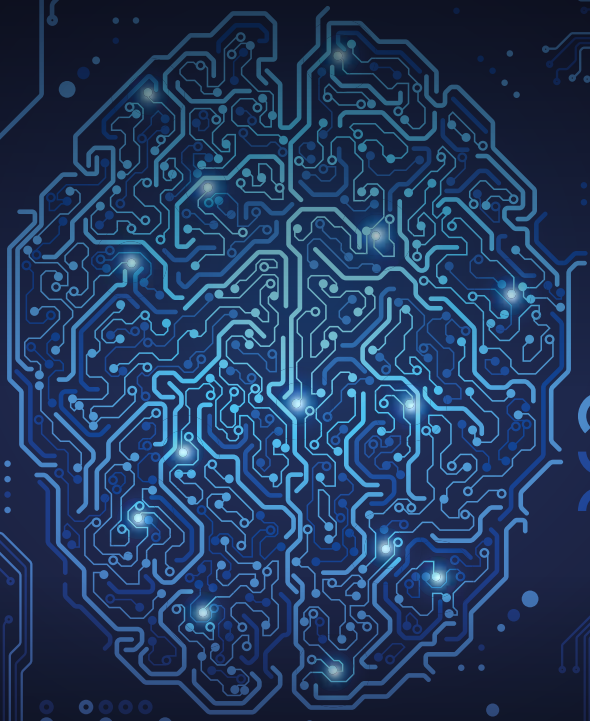
Market
Intelligence

ARTIFICIAL INTELLIGENCE 2021

Global interview panel led by Covington & Burling LLP



LEXOLOGY
Getting the Deal Through

LEXOLOGY
Getting the Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

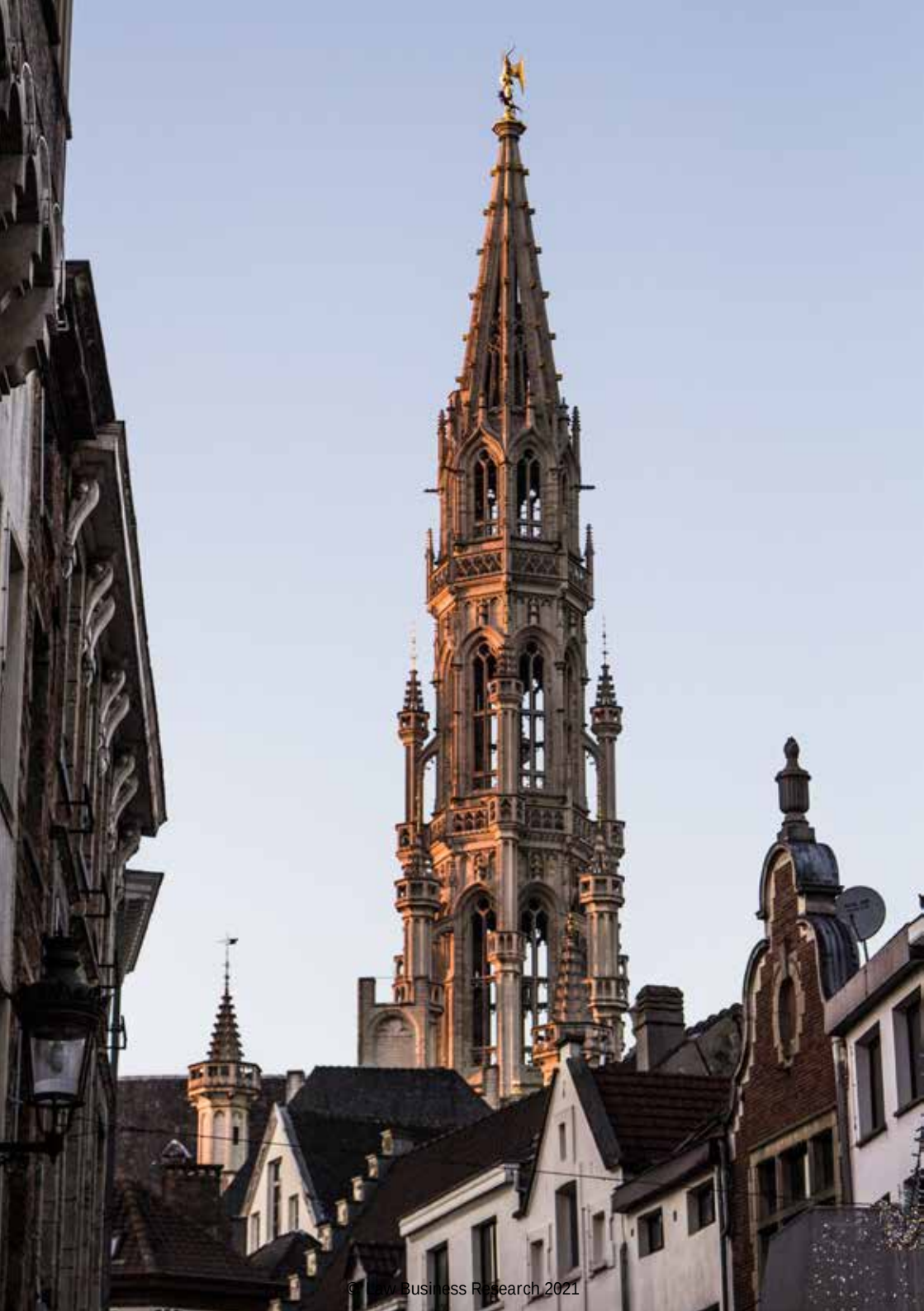
Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/g/
Jakarin+Niamklang

ISBN: 978-1-83862-734-8

Printed and distributed by Encompass Print Solutions

ARTIFICIAL INTELLIGENCE 2021



European Union

Marty Hansen represents several of the world's leading information technology companies on a broad range of technology regulatory issues, including intellectual property, artificial intelligence, law enforcement access, international trade and competition issues. Drawing on over two decades of experience, Marty also represents online services platforms and IT trade associations on a range of electronic commerce, platform and online liability issues.

Lisa Peets leads the technology and media practice in the firm's London office. Ms Peets divides her time between London and Brussels, and her practice embraces regulatory counsel and legislative advocacy. In this context, she has worked closely with leading multinationals in a number of sectors, including some of the world's best-known technology, media and life science companies. Ms Peets counsels clients on a range of EU law issues.

Sam Jungyun Choi is an associate in the technology regulatory group in the London office. Her practice focuses on European data protection law and new policies and legislation relating to innovative technologies. Ms Choi advises leading technology, software and life sciences companies on a wide range of matters relating to data protection and cybersecurity issues.

Jiayen Ong is a trainee solicitor in the London office, who attended Queen Mary, University of London. She has experience across a broad range of practices from competition law, dispute resolution and arbitration, corporate law and technology regulatory issues.

1 What is the current state of the law and regulation governing AI in your jurisdiction? How would you compare the level of regulation with that in other jurisdictions?

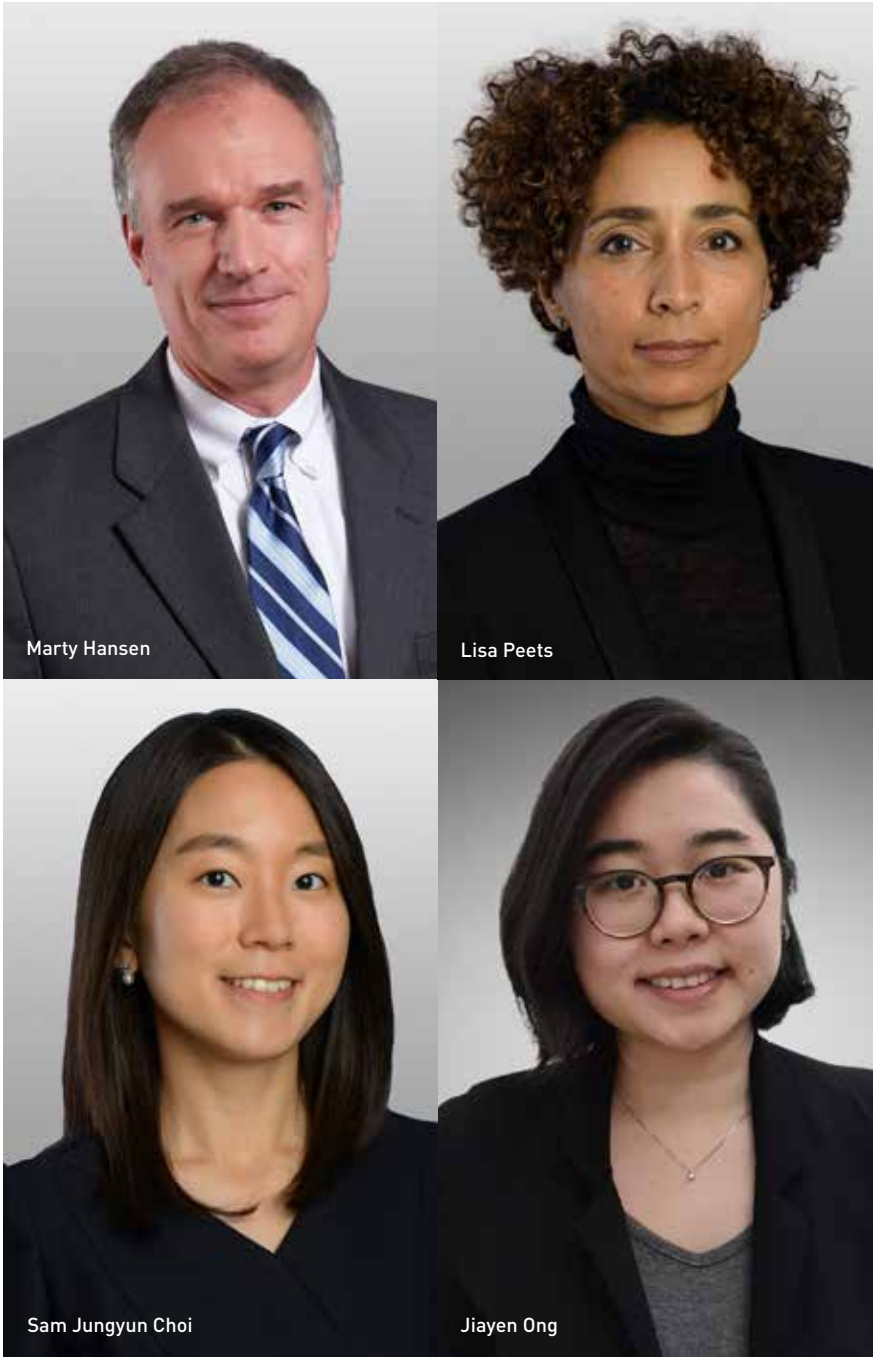
Currently, the European Union does not have laws or regulations that specifically regulate AI. However, a range of laws and regulations – both horizontal and sector-specific – may apply to AI technologies and applications. These include (among others) the following:

- the General Data Protection Regulation (GDPR), which applies to AI applications that process personal data, and imposes heightened obligations on automated individual decision-making, including profiling;
- the Better Enforcement Directive, which requires traders to inform consumers when prices of goods and services have been personalised based on automated decision-making and profiling;
- the Platform-to-Business Regulation, which requires that online intermediation service providers and search engine providers be transparent about the algorithms used to rank business users and corporate websites on its services; and
- the Directive on Copyright in the Digital Single Market, which includes mandatory exceptions to copyright liability for certain acts of text and data mining.

Other laws that may apply to AI applications, depending on the context, include product safety and liability rules, medical devices rules, financial services regulations, cybersecurity laws and consumer protection law.

In April 2021, the European Commission proposed a Regulation Laying Down Harmonised Rules on AI (the AI Act), which would establish rules on the development, placing on the market, and use of AI systems. The AI Act imposes different obligations on providers of different types of AI systems. The bulk of the provisions apply to providers of 'high-risk AI systems'. Prior to placing a 'high-risk AI system' on the EU market or putting it into service, providers are required to undertake a conformity assessment procedure (either self-assessment or third-party assessment) of subject their systems. To demonstrate compliance, providers must draw up an EU declaration of conformity and affix the CE marking of conformity. The AI Act also prohibits certain AI practices that are deemed to pose an unacceptable level of risk, and contravene EU values. The AI Act would also apply to systems, wherever marketed or used, 'where the output produced by the system is used in the Union'. The proposed AI Act is not yet law, and will likely be amended by the Council of the EU and the European Parliament (EP).

Like the EU, the UK has not yet adopted AI-specific legislation. Following the UK's exit from the EU on 1 January 2021, the UK retains some EU laws – such as



the GDPR – by operation of the European Union (Withdrawal) Act 2018. However, the UK government has announced plans to reform UK data protection law. In the UK's National AI Strategy, published in September 2021, the government outlines an innovation-friendly approach to AI regulation that is likely to impose fewer requirements on AI developers and users than are currently set forth in the EU's proposed AI Act. The Office for AI is expected to publish a White Paper on regulating AI in early 2022.

2 | Has the government released a national strategy on AI? Are there any national efforts to create data sharing arrangements?

In 2018, the European Commission published a Coordinated Plan on Artificial Intelligence, which set out a joint commitment by the Commission and the member states to work together to encourage investments in AI technologies, develop and act on AI strategies and programmes, and align AI policy to reduce fragmentation across jurisdictions. In April 2021, the European Commission conducted a review of the progress on the 2018 Coordinated Plan, and set out an updated plan with the following additional policy objectives:

- set enabling conditions for AI development and uptake in the EU;
- make the EU the place where excellence thrives from the lab to market;
- ensure that AI works for people and is a force for good in society; and
- build strategic leadership in high-impact sectors.

The Commission has also proposed that the EU invests at least €1 billion per year from the Horizon Europe and Digital Europe programs in AI. The review found that 19 of the 27 EU member states have adopted national strategies on AI – and the remaining national strategies are in progress and are expected to be published soon.

On data-sharing, in early 2020, the Commission published a communication on shaping Europe's digital future and a European strategy for data. The Communication also recommends enhancing regulatory frameworks to, among other things, encourage data sharing. Over the past year, the European Commission has proposed legislation aimed at furthering the European strategy for data:

- In November 2020, it proposed regulation on European data governance (the Data Governance Act), which aims to promote the reuse of public sector data, introduce regulation targeting data intermediation service providers, encourage data altruism, and establish a European Data Innovation Board.
- In December 2020, it published the proposed Digital Markets Act, which introduces measures to regulate online 'gatekeepers', including how they should

> "The UK government has published its own National AI Strategy."

make available to business users data 'provided for or generated in the context of' the business user's use of the gatekeeper's services.

- In December 2020, it released the EU's cybersecurity strategy for the next decade and proposals for a revised Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) and a Directive on the resilience of critical entities (the Critical Entities Resilience Directive).

As noted in the response to the previous question, the UK government has published its own National AI Strategy. That strategy emphasises the importance of ensuring access to and availability of data. One of the actions included in the AI Strategy is for the UK government to publish a policy framework setting out plans to enable better data availability in the wider economy. This framework will include supporting the activities of data intermediaries, including data trusts, and providing stewardship services between those sharing and accessing data.

3 | What is the government policy and strategy for managing the ethical and human rights issues raised by the deployment of AI?

The Commission's proposed AI Act (discussed in the response to question 1) seeks to address not only health and safety risks posed by AI, but also risks to fundamental rights. Under the proposed AI Act, different sets of obligations apply to different types of AI systems, as follows.

Prohibited AI systems

Some AI applications are prohibited outright. These include the provision or use of AI systems that either deploy subliminal techniques (beyond a person's consciousness) to materially distort a person's behaviour, or exploit the vulnerabilities of specific groups (such as children or persons with disabilities), in both cases where physical or psychological harm is likely to occur. The AI Act also prohibits public authorities from using AI for 'social scoring', where this leads to detrimental or unfavourable treatment in social contexts unrelated to the contexts in which the data was generated, or is otherwise unjustified or disproportionate. Finally, it bans

Photo by Gus Martinie on Shutterstock

law enforcement from using 'real-time' remote biometric identification systems in publicly accessible spaces, subject to limited exceptions (eg, searching for specific potential victims of crime, preventing imminent threats to life or safety, or identifying specific suspects of significant criminal offences).

High-risk AI systems

Certain AI systems are classified as inherently high-risk. These systems are enumerated exhaustively in Annexes II and III of the AI Act, and include AI systems that are, or are safety components of, certain regulated products (eg, medical devices, motor vehicles) and AI systems that are used in certain specific contexts or for specific purposes (eg, for remote biometric identification, for assessing students in educational or vocational training). The AI Act imposes a range of obligations on providers of high-risk AI systems. In particular, providers must design high-risk AI systems to enable record-keeping; allow for human oversight aimed at minimising risks to health, safety, or fundamental rights; and achieve an appropriate level of accuracy, robustness and cybersecurity. Data used to train, validate or test such systems must meet quality criteria, including for possible biases, and be subject to specified data governance practices. Providers must prepare detailed technical documentation, provide specific information to users, and adopt comprehensive risk management and quality management systems. Compliance with these obligations will be assessed through a conformity assessment procedure, and a high-risk AI system must be CE marked for conformity before it can be placed on the EU market. The AI Act also envisages obligations on importers and distributors to ensure that high-risk AI systems have undergone the conformity assessment procedure and bear the proper conformity marking before being placed on the market.

Certain non-high-risk AI systems

The AI Act imposes transparency obligations on certain non-high-risk AI systems. Specifically, providers of AI systems intended to interact with natural persons must develop them in such a way that people know they are interacting with the system, and providers of 'emotion recognition' and 'biometric categorisation' AI systems must inform people who are exposed to them of their nature, and providers of AI systems that generate or manipulate images, audio or video content must disclose to people that the content is not authentic. For other non-high risk AI systems, the AI Act also encourages providers to create codes of conduct to foster voluntary adoption of the obligations that apply to high-risk AI systems.

At the member state level, national strategies have also focused on the ethical and human rights implications of AI. Like the Commission, many member states have established independent bodies tasked with advising on ethical issues raised by

"A number of European data protection authorities have taken an interest in the application of the GDPR to AI."

AI. These include Germany's Data Ethics Commission (which has published ethical guidelines on automated and connected driving and an opinion on AI ethics), the UK's Centre for Data Ethics and Innovation (CDEI), the UK government's Office for AI (which has published guidance on AI Ethics and Safety, guidelines for AI procurement, and public sector-specific guidance), and France's National Consultative Committee for Ethics.

4 What is the government policy and strategy for managing the national security and trade implications of AI? Are there any trade restrictions that may apply to AI-based products?

On 9 September 2021, the EU's recast of the Dual-Use Regulation entered into force. While export controls under the previous EU dual use regulation applied to certain AI-based products, such as those that use encryption software, and any AI products that are specifically designed for a military end use, the updated Dual-Use Regulation broadens the scope of the controls and implements more extensive requirements for cyber-surveillance related goods, software and technology, and

military-related technical assistance activities. That said, while it is a response to new security risks and emerging technology, the new regulation still does not contain AI-specific requirements.

5 How are AI-related data protection and privacy issues being addressed? Have these issues affected data sharing arrangements in any way?

The GDPR applies to all processing of personal data, including in the context of AI systems. This means that AI systems trained on personal data, or processing personal data, falls within the scope of the GDPR. This imposes, among other things, requirements to be transparent about the processing, identify a legal basis for the processing, comply with data subject rights, keep personal data secure, and keep records to demonstrate compliance with the GDPR.

Notably, the GDPR includes specific requirements on fully automated decision-making (ADM) that has legal or similarly significant effects on individuals (article 22). This provision is likely to be particularly relevant to AI-based algorithmic decision-making processes. Under the GDPR, individuals have the right not to be subject to ADM unless the processing is based on the individual's explicit consent, is necessary for performance of a contract between the organisation and the individual, or is authorised by member state or EU law. Even when these conditions are met, organisations must provide individuals with 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing' (article 13(2)(f)). Organisations carrying out ADM must also implement safeguards, including, at a minimum, the right to contest the decision and obtain human review of the decision (article 22(3)). Where sharing personal data between multiple organisations is required to develop or deploy an AI application, the usual rules in the GDPR that apply to data sharing apply. This includes ensuring that any joint controllers of the personal data set out their respective roles and responsibilities for compliance with the GDPR in a transparent way (article 26), and data processing agreements are put in place with processors (article 28). Any cross-border transfers of personal data from within the European Union to outside the EU will also be subject to the usual rules that apply to international data transfers (Chapter V). Further, the development and deployment of AI technologies in certain contexts may also trigger the requirement to carry out a mandatory data protection impact assessment (article 35), which will require organisations to carry out an in-depth review of their data protection compliance specific to the project.

A number of European data protection authorities (DPAs) have taken an interest in the application of the GDPR to AI. The UK Information Commissioner's Office (ICO) has published guidance documents regarding the application of data

protection principles to AI. Other DPAs, including the French CNIL and the Spanish AEPD, have issued guidance on AI and data protection.

6 How are government authorities enforcing and monitoring compliance with AI legislation, regulations and practice guidance? Which entities are issuing and enforcing regulations, strategies and frameworks with respect to AI?

As there is currently no AI-specific legislation in Europe, government authorities do not yet have the power to enforce and monitor compliance with AI-specific legislation.

However, to the extent that existing laws and regulations apply to AI applications, government authorities have been exercising their powers under these rules in relation to AI applications. As noted in question 5, a number of DPAs have been issuing AI-specific guidance in relation to data protection law compliance.

Further, a number of DPAs have recently taken enforcement actions focused on specific AI use cases, particularly relating to facial recognition technology (FRT) used for surveillance purposes. For example, the Swedish DPA in February 2021 fined the Swedish police for using FRT to identify individuals, and in August 2019 fined the Skellefteå municipality for using FRT to track student attendance in a public school. Use of FRT systems by law enforcement for policing and security purposes was also the subject of a human rights challenge before the UK High Court (*R (Bridges) v Chief Constable of South Wales Police* [2019] WLR (D) 496 (UK)) and Court of Appeal (*R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058), and resulted in the UK ICO issuing an opinion on the use of live FRT by law enforcement in public places. In November 2021, the UK ICO and the Office of the Australian Information Commissioner (OAIC) concluded their respective investigations of Clearview AI's facial recognition technologies. Although the ICO has not yet announced its decision, the OAIC has published its determination, which includes a declaration that Clearview AI is required not to repeat or continue practices found to have breached the Australian Privacy Act, and cease collection of and destroy all images collected in contravention of that Act. Since many AI applications involve the processing of personal data, we expect DPAs to play an important role in monitoring AI applications.

On a related note, on 6 October 2021, the EP voted in favour of a non-binding resolution banning the use of FRT by law enforcement in public spaces, which formed part of a non-legislative report on the use of AI by the police and judicial authorities in criminal matters. The EP's report could form the basis of additional EU regulation on the use of AI in law enforcement if the Commission submits a legislative proposal (which could become another AI-specific law within the EU).

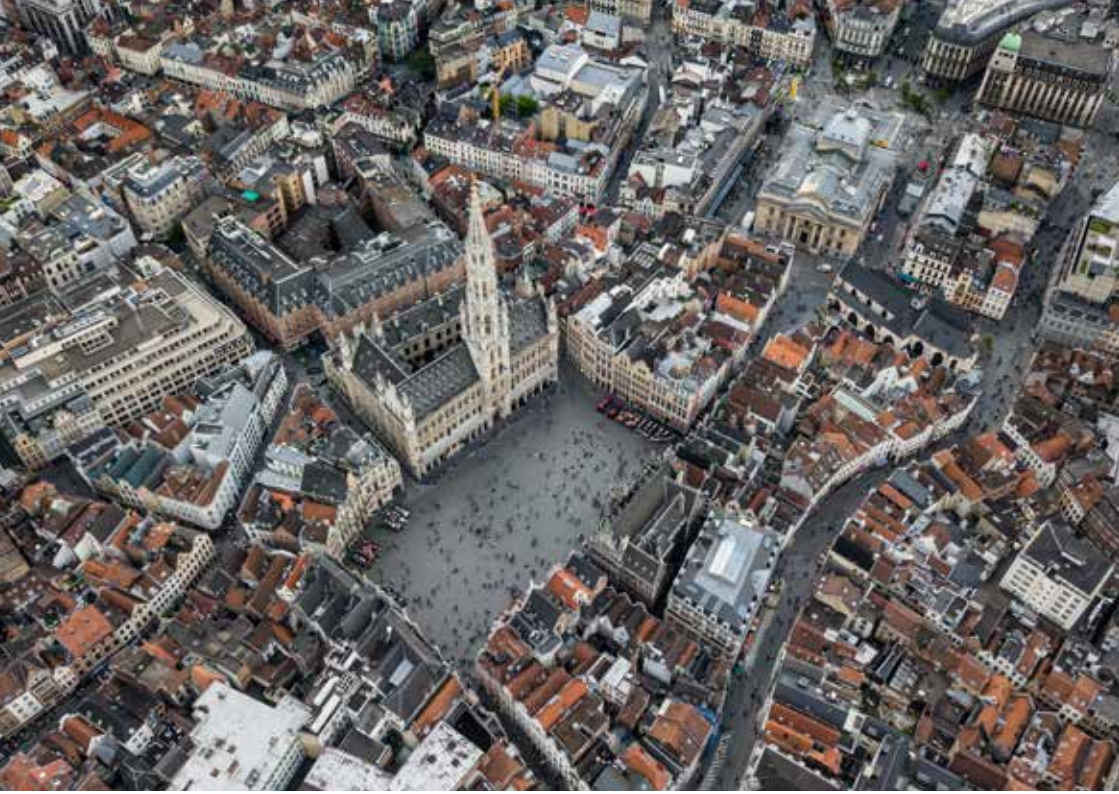


Photo by paxan_semenov on Shutterstock

7 | Has your jurisdiction participated in any international frameworks for AI?

The EU has been a thought leader in the international discourse on ethical frameworks for AI. The AI HLEG's 2019 AI Ethics Guidelines were, at the time, one of the most comprehensive examinations on AI ethics issued worldwide and involved a number of non-EU organisations and several government observers in its drafting. In parallel, the EU was closely involved in developing the OECD's ethical principles for AI and the Council of Europe's recommendation on the human rights impacts of algorithmic systems. At the United Nations, the EU is involved in the report of the High-Level Panel on Digital Cooperation, including its recommendation on AI. The Commission recognises that AI can be a driving force to achieve the UN Sustainable Development Goals and advance the 2030 agenda. The Commission states in its 2020 AI White Paper that the EU will continue to cooperate with like-minded countries and global players on AI, based on an approach that promotes the respect of fundamental rights and European values. Also, article 39 of the Commission's proposed AI Act provides a mechanism for qualified bodies in third countries to carry out conformity assessments of AI systems under the Act.

"Two areas that have seen notable growth in the use of AI-based products are FRT and digital health."

On 1 September 2021, the Commission announced an international outreach for human-centric AI project (InTouchAI.eu) to promote the EU's vision on sustainable and trustworthy AI. The aim is to engage with international partners on regulatory and ethical matters and promote responsible development of trustworthy AI at a global level. This includes facilitating dialogue and joint initiatives with partners, conducting public outreach and technology diplomacy and conducting research, intelligence gathering and monitoring of AI developments. Also, at the first meeting of the US-EU Trade and Technology Council on 29 September 2021, the United States and EU 'affirmed their willingness and intention to develop AI systems that are innovative and trustworthy and that respect universal human rights and shared democratic values'. The participants also established 10 working groups, one of which is tasked with addressing social scoring systems and to collaborate on projects furthering the development of trustworthy AI.

Further, on 3 November 2021, the Council of Europe published a recommendation on data protection in the context of profiling, which is defined as 'any form of automated processing of personal data, including machine learning systems, consisting in the use of data to evaluate certain personal aspects relating to an

individual, particularly to analyse or predict that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.' The recommendation encourages Council of Europe member states to promote and make legally binding the use of a 'privacy by design' approach in the context of profiling, and sets out additional safeguards to protect personal data, the private life of individuals, and fundamental rights and freedoms such as human dignity, privacy, freedom of expression, non-discrimination, social justice, cultural diversity and democracy.

The UK is actively participating in the international discourse on norms and standards relating to AI. It continues to engage with the OECD, Council of Europe, United Nations, and the Global Partnership on AI (GPAI). The UK's National AI Strategy sets out the UK's ambition to create international AI standards to provide an agile and pro-innovation way to regulate AI technologies.

8 What have been the most noteworthy AI-related developments over the past year in your jurisdiction?

The most noteworthy AI-related developments in Europe have been the EU's proposed AI Act and the UK's National AI Strategy, discussed above.

9 Which industry sectors have seen the most development in AI-based products and services in your jurisdiction?

Two areas that have seen notable growth in the use of AI-based products are FRT and digital health. The use of computer vision to power FRT systems for surveillance, identity verification and border control has been a notable development in the EU, raising a number of data protection law-related concerns, as discussed in the response to question 6. The use of other biometric identification systems, such as voice recognition technology, has also proliferated. Such technology can be seen in many forms – from voice authentication systems for internet banking to smart speakers for home use. The digital health sector has seen an increase in AI-powered solutions, including apps that diagnose diseases, software tools for those with chronic diseases, platforms that facilitate communication between patients and healthcare providers, virtual or augmented reality tools that help administer healthcare, and research projects involving analysis of large data sets (eg, genomics data).

10 | Are there any pending or proposed legislative or regulatory initiatives in relation to AI?

As discussed above, the European Commission has published a proposed AI Act. Additionally, the UK government is expected to publish a White Paper on regulating AI in early 2022.

11 | What best practices would you recommend to assess and manage risks arising in the deployment of AI?

Companies developing or deploying AI applications in the EU should be mindful that a number of laws and regulations may apply to their AI application – including, but not limited to, those discussed in the preceding responses. Companies would be well advised to ensure compliance with these laws and look to government authorities that are responsible for enforcement in their sector for any sector-specific guidance on how these laws apply to AI applications. Companies should also closely monitor developments, including legislative proposals following the European Commission's proposed AI Act, and consider participating in the dialogue with policymakers on AI legislation to inform legislative efforts in this area.

Marty Hansen
mhansen@cov.com

Lisa Peets
lpeets@cov.com

Sam Jungyun Choi
jchoi@cov.com

Jiayen Ong
jong@cov.com

Covington & Burling LLP
London
www.cov.com

The Inside Track

What skills and experiences have helped you to navigate AI issues as a lawyer?

At Covington, we take a holistic approach to AI that integrates our deep understanding of technology matters and our global and multi-disciplinary expertise. We have been working with clients on emerging technology matters for decades and we have helped clients navigate evolving legal landscapes, including at the dawn of cellular technology and the internet. We draw upon these past experiences as well as our deep understanding of technology and leverage our international and multi-disciplinary approach. We also translate this expertise into practical guidance that clients can apply in their transactions, public policy matters and business operations.

Which areas of AI development are you most excited about and which do you think will offer the greatest opportunities?

The development of AI technology is affecting virtually every industry and has tremendous potential to promote the public good, including to help achieve the UN Sustainable Development Goals by 2030. For example, in the healthcare sector, AI may continue to have an important role in helping to mitigate the effects of covid-19 and it has the potential to improve outcomes while reducing costs, including by aiding in diagnosis and policing drug theft and abuse. AI also has the potential to enable more efficient use of energy and other resources and to improve education, transportation, and the health and safety of workers. We are excited about the many great opportunities presented by AI.

What do you see as the greatest challenges facing both developers and society as a whole in relation to the deployment of AI?

AI has tremendous promise to advance economic and public good in many ways and it will be important to have policy frameworks that allow society to capitalise on these benefits and safeguard against potential harms. Also, as this publication explains, several jurisdictions are advancing different legal approaches with respect to AI. One of the great challenges is to develop harmonised policy approaches that achieve desired objectives. We have worked with stakeholders in the past to address these challenges with other technologies, such as the internet, and we are optimistic that workable approaches can be crafted for AI.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by Covington & Burling LLP, this *Artificial Intelligence* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Government strategies
Ethics and human rights
Data protection & privacy
Risk & compliance management

ISBN 978-1-83862-734-8