IN-DEPTH

Artificial Intelligence Law

UNITED KINGDOM

LEXOLOGY

Artificial Intelligence Law

EDITION 1

Contributing Editors

Karen Silverman and **Brinson Elliott**

The Cantellus Group

In Depth: Artificial Intelligence Law is a perceptive global overview of the fast-evolving state of law and practice surrounding artificial intelligence (AI) systems and applications. Focusing on recent developments and their practical implications, it examines key issues including legislative initiatives, government policy, AI risk management principles and standards, enforcement actions and much more.

Generated: January 17, 2024

United Kingdom

Gail E Crawford and **Fiona M. Maclean**
Latham & Watkins LLP

Summary

Introduction

The artificial intelligence (AI) industry has experienced significant growth in recent years. The United Kingdom (UK) is estimated to be the third largest AI market in the world, behind the United States and China, with a value of approximately £17 billion in 2022.[2] The private sector is a key driver of this recent growth, particularly in the banking, insurance and business services sectors, and the UK is a leading destination for private AI investment.[3]

The government has expressed a 'pro-innovation' stance on AI, in terms of public funding, technology policy and its regulatory approach.[4] The government is looking to support UK innovation in AI with significant funding for new computing resources, including proposals for a cutting-edge exascale supercomputer that will be capable of training large-scale, complex AI models.[5] This pro-innovation aim is explicit in the government's White Paper on AI regulation, published for public consultation in March 2023 (the AI White Paper),[6] which provides for a principles-based, sectoral and regulator-led framework for the regulation of AI in the UK. The government is expected to further iterate on its proposed regulatory framework, in particular following its headline event – the AI Safety Summit[7] – which took place in early November 2023.[8] In the meantime, AI has become a focus for various UK regulators, including the Information Commissioner's Office (ICO), the Competition and Markets Authority (CMA), Ofcom and the Financial Conduct Authority (FCA), primarily in terms of guidance and policy rather than enforcement at this stage, although enforcement activity by these regulators is very likely on the horizon (the ICO enforcing data protection law in the context of AI systems, for example).

Year in review

i Technology

The AI industry is developing globally, with regional and local divergence driven predominantly by policy and regulatory factors, rather than technical factors. The headline trend of the past year – both globally and in the UK – is the proliferation of accessible generative AI systems. This new world of generative AI has given rise to intense and divisive debate at policy, regulatory and social levels in an array of areas, from individual privacy and the protection of human creativity to existential questions of truth and reality. More recently, enterprise integration has emerged as a key technological shift, as the main providers in the enterprise SaaS (software as a service) and PaaS (platform as a service) markets integrate generative AI systems into their core products. In the UK AI market, generative AI tools are some of the more commonly adopted AI systems, together with data management and analysis solutions, general machine learning tools and AI hardware.[9] Within the generative AI sphere, AI tools for natural language processing and generation are the more commonly adopted and this trend is expected to continue as levels of AI adoption increase across the board.[10] Prevalent use cases for natural language processing and generation AI tools include chatbots and conversational AI (e.g., used in customer service), automated speech or voice recognition and translation tools. Along with generative AI, data management and analysis AI systems top the charts for the most adopted AI across UK businesses,[11] -

] with typical use cases including automated data analytics and predictive insight, database query optimisation and data refinement to improve data quality and accessibility.

ii Developments in policy and legislation

In 2023, the UK government reached a key milestone in its National AI Strategy with the publication in March of its pro-innovation, principles-based AI White Paper for consultation.[12] The government is expected to publish its full response to the AI White Paper consultation by the end of 2023 (following the public consultation phase) and to further iterate on its proposed regulatory framework, although the nature and extent of that development is not yet clear. In recent statements, the government has indicated that it is in no rush to legislate for AI,[13] although it is coming under increasing pressure from several sides to do so (see Section III for further detail). In terms of regulator activity in the AI space, the UK's data protection regulator, the ICO, has been considering the implications of AI since at least 2017 and is continuing to develop guidance and toolkits on various aspects of data protection compliance in an AI context.[14] In recent years, the ICO has been joined by other UK regulators in focusing on AI; for example, the CMA[15] and the FCA[16] have both engaged with industry and other bodies to inform their understanding of AI and its implications. Further, a number of regulators are increasingly coordinating their AI efforts, as exemplified by the AI work by the Digital Regulation Cooperation Forum (DRCF). The DRCF is compromised of the ICO, the CMA, the FCA and Ofcom, and seeks to promote greater collaboration and coherence between those regulators. The group's work on AI includes initiatives in algorithmic processing and its announcement in September 2023 of the DRCF AI and Digital Hub[17] pilot (which is a multi-regulator advisory service for innovators, due to launch in the first half of 2024).

iii Cases

The past year has brought further developments in regulatory enforcement and the commencement of private litigation around AI in the UK. In the regulatory arena, the ICO took action against Clearview AI Inc (a US company that created an AI-powered image database that could be used for facial recognition (Clearview)) in May 2022, alleging (among other matters) a lack of legal basis for the use of personal data and inadequate transparency for individuals.[18] In October 2023, the UK First Tier Tribunal overturned the ICO's 2022 fine and enforcement order against Clearview on jurisdictional grounds.[19] The ICO's action against Clearview, although overturned, is one of a number of challenges to the company's data practices instigated by European data protection regulators.[20-] Also in October 2023, the ICO issued a preliminary enforcement notice against Snap, Inc (a US camera and social media company) and its UK subsidiary for alleged data protection failings in relation to its generative AI chatbot 'My AI'.[21] The ICO's move against Snap follows recent statements expressing limited tolerance for organisations that fail to appropriately consider data protection when developing and implementing AI systems.[22]

In the courts, on 16 January 2023, Getty Images (US), Inc and a number of related entities (Getty) commenced an action against Stability AI Ltd (Stability AI) in the High Court of England and Wales[23] pursuant to which they allege, among other matters, infringement of the copyright in certain artistic works and film works on certain Getty websites and infringement of certain UK registered trademarks.[24] These proceedings are expected to

shed light on intellectual property (IP) subsistence and infringement questions relating to AI models, in particular whether the scraping of images and other works from the internet and the use of such works in training AI models (absent a relevant licence) – especially in generative AI systems – infringes copyright in those works; the extent to which such use falls within fair dealing exceptions under English copyright law; and further whether IP subsists in the output of an AI model. On 2 March 2023, the UK Supreme Court heard the appeal in *Thaler v. Comptroller-General of Patents, Designs and Trade Marks*[25] (*Thaler*), in which the appellant, Dr Stephen Thaler, contended that the inventions in two related patent applications were created by an AI system called the Device for the Autonomous Bootstrapping of Unified Sentience (DABUS), in the absence of a traditional human inventor, and that, as the sole owner, creator and user of DABUS, he is entitled to the rights in inventions claimed in the patent applications.[26] Judgment is reserved following that Supreme Court hearing, with delivery expected later in 2023. The *Thaler* proceedings in the UK form part of a wider campaign by Dr Thale, involving patent applications in a number of jurisdictions,[27] broadly seeking to establish the extent to which an AI system can constitute an inventor of a patent.

Legislative and regulatory framework

The UK government has to date rejected calls to introduce specific legislation targeted at AI systems on the basis that heavy-handed legislation would stifle innovation. Instead, the government's pro-innovation approach is intended to strike a balance between protecting AI users from AI-related harms while ensuring sufficient confidence and clarity for business to innovate responsibly.[28] The proposed regulatory framework, most recently articulated in the AI White Paper, is based on an understanding that individual regulators will be best placed to iterate proportionate and context-driven updates to relevant regulation and guidance to address emerging AI-related harms, based on a series of overarching principles that regulators should take into account when considering developments in their respective sectors:

1. Scope. The UK approach is focused on regulating potentially harmful uses of AI rather than AI systems themselves.[29] AI products and services are identified by reference to two characteristics that are more likely to result in novel risks and regulatory implications: (1) systems that are adaptive to their training, such that the AI system is able to carry out new forms of inference not directly envisioned by its human programmers; and (2) systems that are autonomous in that they are able to make decisions without the express intent or control of a human being.[30]
2. Overarching principles. UK regulators would be required to take into account five principles when responding to AI risks and opportunities in their respective sectors, which are built on the Organisation for Economic Co-operation and Development's principles for responsible stewardship of trustworthy AI:
    - safety, security and robustness;
    - appropriate transparency and explainability;
    - fairness;
    - accountability and governance; and
    - contestability and redress.[31]

Central functions[32] to coordinate, monitor and adapt regulatory frameworks are expected to be developed in due course.

Subsequent to the publication of the AI White Paper in March 2023, there have again been calls by various organisations for the government to consider introducing targeted legislation:

1. Critics argue that a sector-based approach could result in significant gaps in protection for consumers.[33]
2. Regulators are not consistently and appropriately resourced to develop and implement new regulation and guidance.[34]
3. The interim report from the House of Commons Science, Innovation and Technology Committee published in August 2023[35] and the Ada Lovelace Institute report published in July 2023[36] recommend a gap analysis among the UK's regulators to consider whether any of them require new powers to implement and enforce the principles outlined in the AI White Paper, as well as an immediate action to introduce a statutory requirement for regulators to pay due regard to the AI White Paper principles. The July 2023 report from the House of Lords[37] goes a step further and recommends establishing an AI regulator in the medium term. On 22 November 2023, a UK Artificial Intelligence (Regulation) Bill[38] (AI Bill), was introduced to the House of Lords as a Private Member's Bill. The AI Bill proposes, among other matters: (1) the creation of an AI Authority to coordinate sectoral regulators; (2) the mandatory designation of an AI Officer for any business developing, deploying or using AI; (3) an obligation on businesses involved in training AI to provide to the AI Authority a record of all third-party data and IP used in that training, and an assurance that they use all such data and IP with informed consent and in compliance with applicable IP obligations; and (4) a requirement for businesses supplying a product or service involving AI to give users clear and unambiguous health warnings, labelling and opportunities to give or withhold informed consent in advance. The AI Bill is at an early stage in the legislative process, and as a Private Members' Bill, it is unlikely to become binding law (at least not in its proposed form). However, the AI Bill evidences ongoing support from the House of Lords for the creation of specific AI legislation and indicates a potential direction of travel.

The AI White Paper documents the government's intention to pursue a greater degree of collaboration between regulators and the government, to ensure the UK's regulatory framework is practical, coherent and supporting innovation.

Though the UK does not have specific AI legislation, users and developers of AI systems will need to understand and comply with the existing suite of legislation that may apply to a given application of an AI system, in particular in relation to intellectual property, data protection, antitrust and consumer protection.[39] Applicable industry-specific regulation and guidance may also apply to various aspects of the development and use of AI systems (for example, the FCA's Consumer Duty[40] imposes broad obligations on UK-authorised financial services firms in relation to retail customers, including the requirement to 'act to deliver good outcomes for retail customers' with a particular focus on transparency and explainability).

The regulation of AI in the UK is a rapidly evolving space and remains subject to change as various policy pressures come into play, including intense public interest, regulatory scrutiny and competing industry interests.

Managing AI risks and impacts

i Data protection

Legal framework

The UK's data protection framework – primarily comprising the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018[41] – is technology-neutral and applies to any organisation that processes personal data, including using AI systems.

The UK GDPR assigns different compliance responsibilities to controllers (organisations that essentially decide how personal data is used) and processors (organisations that process personal data on behalf of controllers). Controllers have more obligations under the UK GDPR. Of particular relevance when using AI systems, they must:

1. use personal data fairly;
2. ensure that there is a valid lawful basis to process any personal data;[42]
3. inform individuals, in a clear and easy-to-understand way, how their personal data is processed (which poses particular 'explainability' challenges in the AI context);[43]
4. minimise the use of personal data, and ensure that personal data is used only to the extent necessary to fulfil the purpose for which it was collected (which poses practical challenges in relation to large training data sets);[44]
5. design systems to take account of data protection considerations and reduce risk to individuals (privacy-by-design);[45]
6. document and mitigate privacy risks, including via data protection impact assessments (DPIAs) where processing uses new technologies that are likely to result in a high risk to individuals. This may be relevant for many uses of AI systems; for example, as explainability challenges and technical challenges in minimising personal data in training sets or in meeting certain individual rights under the UK GDPR may increase the perceived risk to individuals;[46]
7. keep personal data secure. AI has the potential to drive powerful new cybersecurity and crime prevention solutions but it also introduces new security vulnerabilities (e.g., sophisticated impersonation, bias exploitation, data poisoning);[47] and
8. meet the specific requirements set out in the UK GDPR if the AI system processes personal data without human involvement, and this automated decision-making (ADM) produces legal or similarly significant effects on an individual, including informing the individual and allowing them to object to ADM.[48]

Although the above obligations fall on controllers, the UK GDPR imposes other obligations (such as in relation to data security and contracting) on both controllers and processors. Additionally, processors are restricted from using a controller's data for their own purposes (which could include the further development or training of an AI system for the benefit of other controllers).[49] The ICO recognises the complexities in assigning controller, processor or joint controller roles, especially for processing by AI systems in the cloud, and has indicated it will issue further AI-specific guidance on entities' roles in an AI context.[50]

Regulatory approach and guidance

The ICO has dedicated significant resources to producing specific regulatory guidance on how to comply with data protection law in the context of AI, and has described AI as a 'strategic priority'[51] and an 'area of emphasis',[52] given AI's potential risks to individual privacy.

The ICO's work focuses on the main areas of complexity in the interplay between data protection and AI. Its guidance includes detailed recommendations and expectations on the interaction between AI and ADM and profiling,[53] advice as to the lawful bases of processing at different stages in the AI life cycle (including training and deployment),[54] information about the concept of 'explainability' in AI and its link to UK GDPR transparency obligations,[55] as well as practical guidance[56] and Q&As[57] for developers and users. The ICO has also produced two AI-specific toolkits that map the AI life cycle, related UK GDPR obligations and risks, as well as controls and guidance for compliance.[58]

The ICO has stated that it will continue its work on AI, with an emphasis on:

1. fairness in AI;
2. dark patterns;
3. AI as a service;
4. AI and recommender systems;
5. biometric data and biometric technologies; and
6. privacy and confidentiality in explainable AI.[59]

As well as developing guidance, the ICO is using regulatory tools to encourage compliance, including regulatory sandboxes that provide support to organisations in ensuring specific, innovative processing complies with legal requirements. Sandboxes have been used for a variety of projects, including those relating to AI systems, and practical issues and outcomes have fed into the ICO's AI guidance.[60]

Organisations using AI systems should be aware that other guidance (not specific to AI) may be relevant for data processing, and organisations must in all cases comply with the full suite of UK GDPR obligations. For instance, the UK age-appropriate design code[61] (the AADC), which sets out standards for processing children's data, includes requirements regarding transparency, data minimisation and purpose limitation where AI systems are used for age assurance (e.g., to estimate age based on a person's interactions with services). Furthermore, the AADC notes that controllers conducting DPIAs will need to consider measures to ensure accuracy, avoid bias and explain use of AI.

Enforcement

Non-compliance with the UK GDPR can result in substantial fines of up to the higher of £17.5 million or 4 per cent of annual worldwide turnover[62] or certain enforcement orders,-[63] such as temporary or permanent orders to stop data processing and use of the AI system altogether, or orders to take specific steps to bring data processing into compliance, which could require operational changes to an AI system. The ICO has emphasised that these powers underscore the importance of embedding data protection into the design of AI systems from the outset.[64]

The ICO is a relatively active regulator in this space. In October 2023, it issued a preliminary enforcement notice to Snap, Inc and its UK subsidiary over alleged failures to properly assess the privacy risks posed to children by its generative AI chatbot 'My AI'.[65] If a final enforcement notice is adopted, the ICO could potentially require Snap to cease its data processing in 'My AI' (i.e., effectively turn off the chat bot until the ICO is satisfied that it is operating in compliance with UK data protection law).[66] In May 2022, the ICO issued a £7,552,800 fine[67] and order to stop processing[68] against Clearview. Although both the fine and the enforcement order were overturned in October 2023 on jurisdictional grounds, the ICO's initial decisions shed helpful light on key compliance issues, in particular:

1. legal basis: the ICO initially held that the processing lacked a legal basis for both personal data and biometric data (given the use of facial images constituted biometric data and, therefore, special category data that requires a further condition to be fulfilled under the UK GDPR);[69]
2. fairness and transparency: the ICO found that individuals were not made aware of the processing of their personal data and would not have expected their facial images (which Clearview scraped from the public internet) to be added to Clearview's database for data matching. Furthermore, the processing was effectively invisible to the relevant individuals and Clearview had not provided those individuals with a privacy policy as required by the UK GDPR;[70] and
3. other: the ICO found that Clearview breached other UK GDPR requirements, including that it had no data retention policy,[71] failed to give effect to data subject rights[72] and failed to conduct a DPIA as required by Article 35 of the UK GDPR.

ii Intellectual property

The UK legal principles concerning AI in the context of IP are developing. For the most part, however, IP laws are of general applicability. In the coming years, case law is likely to develop as courts apply existing laws and principles to novel AI-related scenarios (see, for example, the *Thaler* and *Getty* cases referred to above), while the legislature is expected to continue considering the need for any adjustments to the IP legislative framework in light of international developments, among other things. It should also be noted that although the UK post-Brexit has latitude to develop its own IP laws, including with respect to patents, it remains a member of the European Patent Office (EPO) (which is an international organisation rather than an EU body) and a European patent granted by the EPO may cover the UK if so designated in the patent application. Therefore, EPO practice in granting

European patents in the AI space has the potential to affect the UK patent landscape relating to AI inventions.

In relation to copyright protection, the Copyright, Designs and Patents Act 1988 (CDPA) provides for computer-generated work (defined as work generated by computer in circumstances such that there is no human author of the work).[73] Under Section 9 of the CDPA, the author of a literary, dramatic, musical or artistic work that is computer-generated 'shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken';[74] however, it remains to be seen how this provision will be interpreted in the context of AI-assisted (as opposed to AI-generated) work or if the AI inputs (i.e., training data sets) themselves are protected by copyright. Beyond this, for copyright to subsist in a work requires a threshold level of originality – a point that courts will need to grapple with in the context of AI-generated work.

Section 29A of the CDPA includes a limited copyright infringement exemption whereby a person with lawful access to a work makes a copy of a work to carry out a computational analysis of anything recorded in the work for 'the sole purpose of research for a non-commercial purpose'. In June 2022, the government indicated its intention to introduce a new copyright and database right exemption that would have allowed text and database mining (TDM)[75] – which has a significant role in the development and training of AI systems – for any purpose, provided that the party employing TDM obtains lawful access to the relevant material.[76] Importantly, rights holders would not have been able to opt out of this proposed exception or impose specific charges for UK licences for TDM purposes (albeit that rights holders could still choose the platform, or platforms, on which they made their copyrighted work available, and the basis on which they charged for access to those platforms).[77]

Following significant pushback from rights holders, however, the government announced in March 2023 that it would be abandoning this broad TDM exception. Instead, consistent with the Vallance Report[78] recommendations, it indicated its intention to consult with AI firms and rights holders to produce a code of practice (the Code) that supports AI firms to access copyrighted work as an input to their models, while also supporting rights holders by ensuring certain copyright protections (e.g., labelling) for AI-generated output.[79] The government further noted that this non-statutory Code may be followed up with legislation if it is not adopted or agreement is not reached. Working group meetings between the UK Intellectual Property Office and industry representatives from the technology, creative and research sectors commenced in June 2023, though a draft Code has yet to be published.

iii Liability and consumer protection

Overview

Unlike in the European Union, no dedicated legislation has been introduced in the UK that addresses liability or consumer issues in relation to AI in general terms. As such, existing laws will apply. Based on the government's preference for a light-touch approach to AI regulation, the introduction of AI-specific regimes on these issues is unlikely in the near future; however, incremental updates to make existing laws fit for purpose may materialise, and regulators may introduce sector-specific developments.

Heads of liability

Aside from specific considerations such as IP and data protection, there are three main heads of potential general liability in the context of AI.

Statutory liability

The statutory liability framework as it relates to AI is fragmented and, in many cases, uncertain in terms of how and when it is likely to apply.

AI could potentially result in liability under the product liability regime, including the Consumer Protection Act 1987 (CPA); however, it is unclear in what circumstances an AI system or component will meet the definition of a 'product' so as to fall within the scope of that regime. The government has acknowledged that it may be unclear in practice how liability should be attributed under the CPA where AI learns and changes over time,[80] and that recovery is limited to damages for death, personal injury and property and does not extend to immaterial harm (e.g., psychological effects resulting from the use of AI).[81]

From an AI-specific perspective, the Automated and Electric Vehicles Act 2018 introduced statutory liability in a limited context by attributing responsibility for loss to the insurer where damage is caused by an automated vehicle in self-drive mode; however, this is an isolated example of AI-specific statutory liability at this point in time.

Other existing statutory liability regimes are likely to apply in the context of AI albeit the extent to which that will be the case in practice is often unclear. As an example, the potential for the use of AI to result in, or to amplify, discriminatory treatment could result in liability under the Equality Act 2010 (e.g., where the use of AI results in an outcome that is biased in relation to a protected characteristic); however, case law is yet to develop in this context.[82]

Liability for breach of contract

Where there is a contractual relationship between two or more parties regarding AI, there may be a claim for breach of contract (e.g., if the AI malfunctions or fails to perform as promised). This head of liability will not apply to a number of relationships in the AI chain that are unlikely to be governed by a contract (e.g., an end user may have no contract with the original developer or distributor of an AI system). Contractual liability depends on a range of factors but the following are of particular interest in an AI context.

Contract terms

1. Express terms: Although market practice is developing and varies by context, in the business-to-consumer environment, contracts with leading AI providers generally do not contain many express warranties or commitments in favour of purchasers or users that would give grounds for contractual claims if breached. Providers also typically disclaim or exclude a broad range of potential liabilities, although English law imposes limitations on that approach. A more customer-friendly approach appears to be emerging in the business-to-business environment, at least in relation to liability for intellectual property infringement, as evidenced by commitments from

a number of market-leading enterprise AI providers to indemnify their customers against IP infringement claims.[83]

2. Implied terms: Nevertheless, certain terms may be implied by law into contracts regarding AI, including under consumer law.[84] The CMA has confirmed that digital content created using an AI foundation model may come within the remit of the Consumer Rights Act 2015, which would result in implied terms in consumer contracts that AI is of satisfactory quality, fit for purpose and as described.[85] Implied terms under the Sale of Goods Act 1979 may apply to business-to-business contracts, although it is not yet clear in what circumstances AI will constitute a 'good' or part of a 'good', so as to fall within the scope of that regime. In summary, although implied terms will apply in certain cases, many contracts relating to AI are likely to be substantially free from such terms.

Causation

1. Factual causation: To the extent that an AI system is a 'black box', such that it is not possible to fully examine the underlying code or logic, factual causation (i.e., the question of which act, or omission, caused an output that resulted in a loss) may be difficult to ascertain or prove. This challenge may be exacerbated by the multiplicity of actors in an AI supply chain, which may include an original developer, a commercial provider, a support provider, the end user, among others. For instance, even if it is established that a fault in the AI algorithm resulted in a loss, there may be a dispute about whether that fault was caused by the original developer or by a third-party support provider that subsequently patched or updated that algorithm.
2. Legal causation: For damages to be recoverable under a breach of contract claim, it must generally be demonstrated that the loss is not too remote as to be considered unrecoverable (i.e., legal causation). Particularly in the case of AI solutions capable of use in a range of different contexts (i.e., general purpose models), it is unclear how readily that burden may be overcome as, by design, these models are intended to be used for purposes that are not necessarily foreseen at the point of development.

Liability under tort

Claimants may seek to rely on tortious liability and, in particular, negligence claims. This is particularly likely if claimants do not benefit from substantial contractual commitments from the other party, or there is no contractual relationship (e.g., if an end user seeks recovery from a party further up the AI chain, such as the original developer). It is currently unclear to what extent the courts will be willing to extend a duty of care to the developers or providers of an AI model, or what the relevant duty of care would be (i.e., the standard to be met to avoid liability). In addition, many of the challenges regarding causation noted above will apply in a similar manner to negligence claims.

Managing and apportioning liability

There are a number of contractual, operational and other measures that parties can – and increasingly do – leverage to manage and apportion liability regarding AI.

Contractual mechanisms

Developers and providers of AI often issue prescriptive terms of use, instruction manuals or similar, which set out the parameters of how the AI should be used (e.g., which inputs should be avoided or are prohibited and a list of purposes or use cases for which the AI cannot be relied on). If end users breach such terms (even if not contractually binding), the developer or provider may have an argument that the end user – rather than the developer or provider – caused any resulting loss (in other words, such terms help to address the issues regarding causation noted above).

AI providers often seek to include broad disclaimers and exclusions of liability in their standard contract terms, including that (subject to limited exceptions) the AI is provided as is (particularly for general purpose models), no commitment is made regarding suitability for any specific purpose, and that liability for a broad range of losses is excluded. Although such terms can be effective, their use is subject to certain limitations under English law,[86] in particular in a consumer context.[87]

It is open to purchasers of AI, particularly in agreements for bespoke AI (as the purchaser is likely to have more negotiating leverage), to seek express representations, warranties and other commitments to clarify that the provider remains liable for certain losses (e.g., a warranty regarding fitness for a specific purpose, where the AI has been developed for a specific use case). Many purchasers also seek a general obligation on the provider to comply with applicable laws, although there can be reluctance to grant that given the uncertainties regarding the applicability of current law in an AI context and the potential for future developments.

Operational and other mechanisms

Providers and users of AI can limit liability exposure by regularly testing the functionality of the AI and keeping clear records of such tests, including any remediation measures implemented.[88]

Providers and users can further limit exposure by including a 'circuit breaker', allowing them immediately to pause the operation of the AI system or allowing a function to 'roll back' the AI to an earlier iteration.[89]

The insurance market is still developing in terms of AI; however, it is likely to play an increasing part in mitigating and apportioning risk.

Enforcement

There is currently minimal AI-specific enforcement in the UK. However, see 'Enforcement' under Section IV.i, above, regarding data protection, and Section IV.ii on intellectual property.

Legal practice implications

Since the surge in generative AI, there has been an influx of new AI and generative AI-based legal technology (legal tech) in the UK, European and global markets, adding to the first wave of earlier AI legal technology. General AI applications – not specific for the legal market – are also used widely in a legal context, though demand for legal practice-specific AI tools is high, given the particular demands of the legal market (such as high standards for accuracy, explainability and information security, and the specific nature of legal practice use cases).

Along with other professional services, the legal vertical has been among the first to experience significant growth in AI tools, in this latest wave of powerful AI systems,[90] in part due to the large number of activities across legal practice that can be accomplished more efficiently or more effectively by AI, and the fact that those activities are typically relatively high value. These characteristics result in a market that is ripe for industry-specific AI innovation. AI legal tech is growing across nearly all areas of the legal market, from contentious practices to advisory and commercial matters. Similarly, AI tools are proliferating on both the client-facing side (from contract drafting and due diligence to legal research, discovery and court ruling predictions) and on the legal practice management and operations side (in areas such as fees and financing, knowledge management and document management).

There are certain barriers to change within the AI legal tech market, in the UK and elsewhere, including challenges in achieving frictionless end-to-end AI legal processes. AI legal tools typically address inefficiencies in a particular task or stage of a legal process (e.g., reviewing a document, documenting changes to a document, or simultaneously amending a large number of documents) but do not address the process end-to-end or with interoperability. This leaves certain residual inefficiencies and bandwidth issues in the process as a whole. Further, there is a lack of common standards in information security (particularly in relation to cloud technology) across the various participants in the legal market, which hinders rapid and wide adoption of AI. In addition, multi-sided or multi-party AI legal tech requires a critical mass of engagement for the technology to supersede the previous, off-tech process. It may take a while for the latest wave of AI legal tech to achieve that critical mass in the UK and global legal markets, but AI tools look set to be ultimately transformative across legal practice.

Outlook and conclusions

The AI market in the UK is expected to maintain its growth trajectory during the coming year and beyond, as AI technologies develop further towards a state of artificial general intelligence and enterprise integration of generative AI tools continues at pace. Deep learning and natural language processing are predicted to experience relatively high rates of growth – and material technological advances – and to collectively account for the majority of the UK AI market in the short to medium term.[91] During the next few years, industry growth and investment in the AI space is expected to be concentrated in the banking, insurance and business services sectors (which are currently driving much of the UK AI market), as well as the retail and manufacturing sectors.[92] Healthcare, autonomous vehicles and intelligent transportation are also potential areas of significant future AI advancement and market investment, both in the UK and at a global level. Looking further

ahead, the drivers for AI adoption are likely to widen from efficiency gains and automation to more sophisticated deployment to meet complex technical and commercial challenges.

A key technological development on the horizon is the government's proposed cutting-edge exascale supercomputer, which will be capable of training large-scale, complex AI models.-[93] The exascale system will sit alongside two new supercomputers to be built in the UK, Isambard-AI and Dawn,[94] and together they will form the national AI Research Resource, which is intended to support the work of the AI Safety Institute[95] and the Frontier AI Taskforce[96] and to facilitate exponential progress in AI innovation and safety in the UK.

The fast pace of innovation and the increasingly sophisticated nature of AI adoption is expected to drive further development of the government's regulatory framework for AI. The extent of that development is not yet clear, though the government has indicated that it is in no rush to legislate for AI.[97] It seems unlikely, therefore, that the government will table comprehensive AI legislation at this stage, but it may be that it seeks to put the AI principles set out in the AI White Paper on a statutory footing. In parallel, regulatory scrutiny of AI is expected to increase and may shift into more active enforcement during the coming year, particular in the spheres of data protection, consumer and antitrust. Further, AI standards are likely to take a more prominent role in AI governance and compliance, as global technical standards continue to be developed, resulting in an increasingly more consistent and efficient global framework of AI standards.[98] Finally, cybersecurity is expected to be a key challenge in the AI space, as cyber innovation (including AI-driven innovation) and industry standards ramp up to meet emerging cyber risks and AI-specific cyber vulnerabilities.

Endnotes

1. Gail Crawford and Fiona Maclean are partners at Latham & Watkins LLP. The authors would like to acknowledge the kind assistance of their colleagues Calum Docherty, Georgina Hoy, Edgar Lee, Ben Leigh, Lorenzo Meusburger, Brett Shandler, Alain Traill, Nara Yoo and Amy Smyth with the preparation of this chapter. ^ Back to section

2. United States International Trade Administration, Market Intelligence, 'United Kingdom Artificial Intelligence Market' (September 2022), available at https://www.trade.gov/market-intelligence/united-kingdom-artificial-intelligence-market-0#:~:text=The%20UK's%20AI%20market%20is. ^ Back to section

3. In 2022, the United Kingdom (UK) was ranked third in the world as a destination for private AI investment: see Daniel Zhang, et al., 'The AI Index 2022 Annual Report', AI Index Steering Committee, Stanford Institute for Human-Centered AI (Stanford University, March 2022). ^ Back to section

4. As set out in the UK National AI Strategy, available at https://www.gov.uk/government/publications/national-ai-strategy. ^ Back to section

5. The government has allocated £900 million to build the exascale supercomputer and more broadly uplift the UK's computing capacity (see 'Outlook and conclusions', below, for further detail). ^ Back to section

6 Department for Science, Innovation & Technology and Office for Artificial Intelligence, 'A pro-innovation approach to AI regulation' (2023) (the AI White Paper), available at https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#executive-summary. ^ Back to section

7 The AI Safety Summit 2023 took place on 1 and 2 November 2023 at Bletchley Park in the UK and brought together the UK and other governments and regulators, academics and executives from a number of leading AI companies. The summit considered the potential risks and safety aspects of AI, and how those risks can be mitigated through coordinated, international action. Further information is available at https://www.gov.uk/government/topical-events/ai-safety-summit-2023. ^ Back to section

8 A number of significant steps were announced immediately following the AI Safety Summit, including the signing of the 'Bletchley Declaration on AI Safety' by multiple countries committing to collaborate to identify and build understanding of AI safety risks, and the establishment of the AI Safety Institute as a global hub for collaboration between governments and various AI companies on testing the safety of emerging AI technologies. ^ Back to section

9 Capital Economics report (commissioned by the UK government), 'AI Activity in UK Businesses' (January 2022), available at https://www.gov.uk/government/publications/ai-activity-in-uk-businesses. The report provides that 9 per cent of UK businesses have adopted data management and analysis AI solutions, 8 per cent have adopted natural language processing and generation solutions, followed by machine learning (7 per cent adoption), AI hardware (5 per cent adoption), and computer vision and image processing and generation (5 per cent adoption). ^ Back to section

10 ibid. The Capital Economics report provides that 85 per cent of UK businesses that are planning to adopt AI solutions in the future intend to adopt natural language processing and generation AI systems, which follows closely behind the intended adoption of data management and analysis AI systems (89 per cent of UK businesses planning to adopt AI solutions in the future). ^ Back to section

11 ibid. ^ Back to section

12 The AI White Paper is covered in detail in 'Legislative and regulatory framework', below. ^ Back to section

13 During a speech hosted by think tank Onward in October 2023, Michelle Donelan, UK Secretary of State for Science, Innovation and Technology, said: 'We are not afraid to legislate but what we are saying is that we shouldn't be rushing to implement very fixed solutions before we properly understand the problem.' And further: 'But our . . . way forward in this country is not to rush to legislate when we don't know all the answers yet.' As reported by Politico on 24 October 2023. ^ Back to section

14 The work by the Information Commissioner's Office (ICO) on data protection and AI includes an 'AI and data protection risk toolkit', a 'data analytics toolkit' and detailed guidance on explaining decisions made with AI (co-authored with The Alan Turing Institute). ^ Back to section

15 In September 2023, the Competition and Markets Authority (CMA) published a report on foundation models, including a set of proposed principles to guide competitive AI markets and protect consumers (available at https://www.gov.uk/government/news/proposed-principles-to-guide-competitive-ai-markets-and-protect-consumers) and in parallel launched a wide-ranging programme of engagement with industry and other stakeholders to inform further development of the proposed AI principles. ^ Back to section

16 On 26 October 2023, the Financial Conduct Authority (FCA), with the Bank of England and the Prudential Regulation Authority, published Feedback Statement 2/23 (https://www.bankofengland.co.uk/prudential-regulation/publication/2023/october/artificial-intelligence-and-machine-learning) in response to the October 2022 joint Discussion Paper titled 'Artificial Intelligence and Machine Learning' (DP5/22). DP5/22 and FS 2/23 form part of those regulators' engagement with the financial services industry on AI, including the AI Public-Private Forum (AIPPF), which ran from October 2020 to October 2021 to establish dialogue between the public and private sectors on the uses and impacts of AI in financial services, culminating in the AIPPF's Final Report (https://www.bankofengland.co.uk/research/fintech/ai-public-private-forum). ^ Back to section

17 More information available at https://www.drcf.org.uk/publications/blogs/ai-and-digital-regulations-hub. ^ Back to section

18 See the ICO's 18 May 2022 Monetary Penalty Notice addressed to Clearview AI Inc (https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-20220518.pdf) and the ICO's 18 May 2022 Enforcement Notice addressed to Clearview AI Inc (https://ico.org.uk/media/action-weve-taken/enforcement-notices/4020437/clearview-ai-inc-en-20220518.pdf). ^ Back to section

19 See*Clearview AI Inc v. The Information Commissioner* [2023] UFTT 00819 (GRC). It is open to the ICO to appeal the court's decision. ^ Back to section

20 Data protection regulators in the following jurisdictions have also taken action against Clearview: Austria, France, Germany, Greece, and Italy. ^ Back to section

21 See the ICO news release (https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/uk-information-commissioner-issues-preliminary-enforcement-notice-against-snap/). ^ Back to section

22 For example, on 3 April 2023, the ICO published a statement including the following: 'There really can be no excuse for getting the privacy implications of generative AI wrong', and 'We will act where organisations are not following the law and considering the impact on individuals.' (https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/. ^ Back to section

23 Case No. IL2023000007. ^ Back to section

24 The Getty claimants seek relief (including injunctive relief) and an inquiry as to damages or an account of profits. Pursuant to a consent order dated 28 September 2023, the proceedings will now move to an interlocutory hearing, for parties to call expert and fact evidence to address technical issues relating to the development, training and testing of generative AI models, including that of Stability AI's Stable Diffusion. The interlocutory hearing is likely to take place by the end of 2023, with a trial date for the main proceedings expected within the coming year. ^ Back to section

25 *Thaler (Appellant) v. Comptroller-General of Patents, Designs and Trade Marks (Respondent)* UKSC [2021/0201]. ^ Back to section

26 For the purpose of the*Thaler* proceedings, it has been assumed that the Device for the Autonomous Bootstrapping of Unified Sentience (DABUS) is the deviser of the inventions claimed in the patent applications. Prior to the UK Supreme Court hearing, Dr Thaler's appeal of the Comptroller-General's decision to refuse to accept Dr Thaler's designations of DABUS as the inventor in the patent applications under Section 13 of the Patents Act 1977 was dismissed in both the High Court and the Court of Appeal of England and Wales. ^ Back to section

27 Including (among others) Australia, the European Patent Office, Germany, South Africa and the United States. ^ Back to section

28 Select Committee on Artificial Intelligence, Report of Session 2017–19: 'AI in the UK: ready, willing and able?' (HL 2017-19, 100). ^ Back to section

29 The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (issued by The White House in October 2023) has a broadly similar focus on potentially harmful uses of AI, including specific requirements for large AI models and associated large computing clusters meeting defined thresholds (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/). ^ Back to section

30 This contrasts with the European Union's draft Artificial Intelligence Act's risk-based approach to defining AI systems, which categorises them by their apparent risk to individuals, with a list of prohibited use cases being categorised as 'unacceptable', 'high risk' use cases being subject to the strictest requirements, while 'low' and 'minimal risk' use cases are likely to face a lower regulatory burden: see European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', COM(2021) 206 final, 21 April 2021. ^ Back to section

31 Organisation for Economic Co-operation and Development, 'Recommendation of the Council on Artificial Intelligence' (OECD/LEGAL/0449) (2003). ^ Back to section

32 The AI White Paper identifies a set of functions that the government seeks to coordinate centrally to facilitate collaboration and drive regulatory coherence, including a monitoring and assessment function, a cross-sectoral risk assessment function, an education and awareness function, and a horizon scanning function. The government states in the AI White Paper that it will initially be responsible for delivering these central functions, working in partnership with regulators and other stakeholders in the AI ecosystem. Looking to the longer term, the government states that it recognises that there may be value in a more independent delivery of the central functions. ^ Back to section

33 For example, a job applicant, on receiving a negative decision because of an AI algorithm's bias against regional accents may not be adequately protected under current equality or human rights legislation as this is not a protected characteristic. ^ Back to section

34 For example, certain regulators such as the FCA, the CMA, Ofcom and the ICO already cooperate – including on AI topics - through forums such as the Digital Regulation Cooperation Forum, whereas others, such as the Human Rights Commission, have much more limited experience, capacity and access to AI expertise. ^ Back to section

35 House of Commons Science, Innovation and Technology Committee, 'The governance of artificial intelligence: interim report' (August 2023), available at https://publications.parliament.uk/pa/cm5803/cmselect/cmsctech/1769/report.html. ^ Back to section

36 Ada Lovelace Institute, Report, 'Regulating AI in the UK' (July 2023), available at https://www.adalovelaceinstitute.org/report/regulating-ai-in-the-uk/. ^ Back to section

37 House of Lords Library, 'Artificial intelligence: Developments, risks and regulation' (18 July 2023), available at https://lordslibrary.parliament.uk/artificial-intelligence-development-risks-and-regulation/. ^ Back to section

38 Available at https://bills.parliament.uk/publications/53068/documents/4031. ^ Back to section

39 For example, an AI tool for assessing the credit-worthiness of loan applicants could fall within the remit of the ICO (use of personal data), the FCA (provision of financial services) and the Equality and Human Rights Commission (in the event of potentially discriminatory treatment based on protected characteristics, such as race or gender).- ^ Back to section

40 Further information available at https://www.fca.org.uk/firms/consumer-duty. ^ Back to section

41 Another key part of the UK's data protection framework is the Privacy and Electronic Communications Regulations 2003, which imposes obligations for marketing, tracking technologies, communications services and user privacy in respect of traffic and location data. At the time of writing, this has not been a key focus in terms of AI-specific compliance. ^ Back to section

42 UK GDPR, Articles 6 and 9. ^ Back to section

43 id., Articles 5(1)(a), 13 and 14. ^ Back to section

44 id., Article 5(1)(c). ^ Back to section

45 id., Article 25. ^ Back to section

46 id., Article 35. ^ Back to section

47 id., Article 5(1)(f). ^ Back to section

48 id., Articles 13(2)(f), 14(2)(g) and 22. ^ Back to section

49 Note there is a legal minimum set of obligations that processors are required to undertake to controllers contractually, set out in UK GDPR, Article 28. ^ Back to section

50 ICO, 'Guidance on AI and data protection', available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/. ^ Back to section

51 See ICO response to the AI White Paper, available at https://ico.org.uk/media/about-the-ico/consultation-responses/4024792/ico-response-ai-white-paper-20230304.pdf. ^ Back to section

52 See 'Information Commissioner's Annual Report and Financial Statements 2022/23', available at https://ico.org.uk/media/about-the-ico/documents/4025864/annual-report-2022-23.pdf. ^ Back to section

53 ICO, 'What is automated decision-making and profiling?', available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/. ^ Back to section

54 ICO, 'How to use AI and personal data appropriately and lawfully', available at https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf; see also ICO, 'Guidance on AI and data protection', available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/. ^ Back to section

55 ICO and The Alan Turing Institute, 'Explaining decisions made with AI', available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/. ^ Back to section

56 ICO, 'Big data, artificial intelligence, machine learning and data protection', available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. ^ Back to section

57 ICO blog post, 'Generative AI: eight questions that developers and users need to ask', available at https://ico.org.uk/about-the-ico/media-centre/blog-generative-ai-eight-questions-that-developers-and-users-need-to-ask/. ^ Back to section

58 ICO, 'AI and data protection risk toolkit', available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/; and 'Toolkit for organisations considering using data analytics', available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/toolkit-for-organisations-considering-using-data-analytics/. ^ Back to section

59 ICO summary of its work on AI, available at https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/. ^ Back to section

60 See ICO, 'Regulatory Sandbox beta review' at Section 3 (available at https://ico.org.uk/media/for-organisations/documents/4019035/sandbox-beta-review.pdf) in relation to Onfido sandbox. ^ Back to section

61 ICO, 'Age appropriate design: a code of practice for online services' (October 2022), available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. ^ Back to section

62 UK GDPR, Articles 83, paragraphs (4) to (6). ^ Back to section

63 id., Article 58(2). ^ Back to section

64 ICO statement, 'Don't be blind to AI risks in rush to see opportunity – ICO reviewing key businesses' use of generative AI', available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/06/don-t-be-blind-to-ai-risks-in-rush-to-see-opportunity/. ^ Back to section

65 See the ICO's announcement, available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/uk-information-commissioner-issues-preliminary-enforcement-notice-against-snap/. ^ Back to section

66 ibid. ^ Back to section

67 See the ICO's 18 May 2022 Monetary Penalty Notice addressed to Clearview AI Inc, op. cit. note 18. ^ Back to section

68 See the ICO's 18 May 2022 Enforcement Notice addressed to Clearview AI Inc, op. cit. note 18. ^ Back to section

69 UK GDPR, Articles 6 and 9. ^ Back to section

70 The ICO found a number of breaches of the UK GDPR's fairness and transparency requirements, including under UK GDPR, Article 5(1)(a) and GDPR, Article 14. ^ Back to section

71 Required to implement the principle of storage limitation under UK GDPR, Article 5(1)(e). ^ Back to section

72 The data subject rights that were breached include those under UK GDPR, Articles 15, 16, 17, 21 and 22. ^ Back to section

73 Copyright, Designs and Patents Act 1988 (CDPA), Section 178. ^ Back to section

74 Copyright law (under the CDPA) and patent law (under the Patents Act 1977) are therefore similar in their requirement for a human owner of the intellectual property rights (i.e., the AI system itself cannot be treated as an author, owner or inventor (as relevant)). This requirement is currently being challenged in relation to patent protection in the *Thaler* case. ^ Back to section

75 Text and database mining is the use of automated computational techniques to analyse large amounts of information to identify patterns, trends and other useful information. ^ Back to section

76 GOV.UK, Intellectual Property Office, Consultation outcome: 'Artificial Intelligence and Intellectual Property: copyright and patents: Government response to consultation' (28 June 2022) available at https://www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/outcome/artificial-intelligence-and-intellectual-property-copyright-and-patents-government-response-to-consultation. ^ Back to section

77 As part of the same June 2022 response, the UK government indicated that it did not consider that changes to the law were necessary to amend or remove copyright protection for computer-generated works without a human author, or to allow for patent protection for AI-devised inventions, but would keep the law on these points under review. ^ Back to section

78 Report presented by Sir Patrick Vallance, 'Pro-innovation Regulation of Technologies Review: Digital Technologies' (March 2023), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142883/Pro-innovation_Regulation_of_Technologies_Review_-_Digital_Technologies_report.pdf (Vallance Report). ^ Back to section

79 HM Government, 'HM Government Response to Sir Patrick Vallance's Pro-Innovation Regulation of Technologies Review: Digital Technologies' (March 2023) available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142798/HMG_response_to_SPV_Digital_Tech_final.pdf. ^ Back to section

80 UK Department for Business & Trade, 'Smarter Regulation: UK Product Safety Review' (August 2023), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175948/uk-product-safety-review-consultation-august-2023.pdf. ^ Back to section

81 UK Office for Product Safety & Standards, 'Study on the Impact of Artificial Intelligence on Product Safety: Final Report' (December 2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1077630/impact-of-ai-on-product-safety.pdf. ^ Back to section

82 Forthcoming developments in statutory liability may also touch upon AI, such as the Digital Markets, Competition and Consumers Bill, which will introduce a range of consumer law reforms and may clarify the application of consumer law to AI, in addition to setting 'conduct' requirements for firms with 'strategic market status' in relation to digital activities (this is likely to encompass certain leading providers of AI. See the explanatory notes to the Digital Markets, Competition and Consumers Bill, introduced in the House of Commons on 25 April 2023 (Bill 294), available at https://publications.parliament.uk/pa/bills/cbill/58-03/0294/en/220294en.pdf. ^ Back to section

83 Both Microsoft and Google have committed to indemnifying their enterprise customers of certain of their services against third-party intellectual property claims arising from use of the provider's integrated AI tools, including use of AI-generated outputs (subject to certain limitations in each case). ^ Back to section

84 Consumer law applies to certain interactions with consumers. The term 'consumers' is defined in various ways under different legislation but generally means an 'individual acting for purposes that are wholly or mainly outside that individual's trade, business, craft or profession' (see, e.g., Consumer Rights Act (CRA), Section 2(3)). ^ Back to section

85 CRA, Sections 34 to 36. ^ Back to section

86 For instance, for business-to-business contracts, the Unfair Contract Terms Act 1977 contains a blanket prohibition on exclusions or limitations of liability for negligence resulting in death or personal injury (Section 2(1)). In addition, if contracts are entered into on a provider's standard terms, any provision limiting or excluding liability for breach of contract or non-performance will be subject to a 'reasonableness test' and will be unenforceable if that test is not met (Section 11). ^ Back to section

87 For example, the enhanced consumer protections under the CRA (e.g., Sections 62(4) and 62(6)). ^ Back to section

88 This is likely to be helpful not only in defending negligence claims (as these activities may help to demonstrate that any applicable duty of care has been met) but also for disputes regarding causation (e.g., if tests demonstrate that AI performed appropriately when provided to the purchaser, this may indicate that any issues were caused by subsequent, third-party updates). ^ Back to section

89 These steps may enable the parties to react to unexpected changes in the interpretation of law or regulation, or to limit potential losses where an updated version of the AI is found to result in problematic outputs. ^ Back to section

90 In the UK specifically, research commissioned by the government in 2022 found that the legal sector had the second highest rate of AI adoption (at 29.2 per cent), falling just behind the information technology and telecommunications sector (at 29.5 per cent) – Capital Economics study and report, 'AI Activity in UK Businesses' (January 2022) available at https://www.gov.uk/government/publications/ai-activity-in-uk-businesses/ai-activity-in-uk-businesses-executive-summary. ^ Back to section

91 Apollo Reports, European Artificial Intelligence Market (June 2023), available from Apollo Research Reports at https://www.apollorr.com/. ^ Back to section

92 International Data Corporation, 'Worldwide Artificial Intelligence Spending Guide' (version 1, 2023), available at https://www.idc.com/getdoc.jsp?containerId=IDC_P33198. ^ Back to section

93 The government has allocated £900 million to build the exascale supercomputer, and more broadly uplift the UK's computing capacity: see https://www.gov.uk/government/news/game-changing-exascale-computer-planned-for-edinburgh#:~:text=This%20new%20UK%20government%20funded,and%20clean%20low%2Dcarbon%20energy. ^ Back to section

94 The Isambard-AI and Dawn supercomputers are expected to be operational by the summer of 2024: see https://www.gov.uk/government/news/technology-secretary-announces-investment-boost-making-british-ai-supercomputing-30-times-more-powerful. ^ Back to section

95 The AI Safety Institute was announced at the AI Safety Summit held in the UK in November 2023 as a global hub for collaboration between governments and various AI companies on testing the safety of emerging AI technologies (see 'Year in review, above). ^ Back to section

96 The Frontier AI Taskforce is an expert group within the government, tasked with building an AI research team to evaluate risks at the frontier of AI: see https://www.gov.uk/government/publications/frontier-ai-taskforce-first-progress-report/frontier-ai-taskforce-first-progress-report. ^ Back to section

97 See footnote 13. ^ Back to section

98 AI governance is itself emerging as a new market sector: researchers predict that the global AI governance market will grow from just over US$200 million in 2023 to more than U$700 million by 2028: Mordor Intelligence, 'AI Governance Market Analysis' (2023–2028). ^ Back to section

LATHAM & WATKINS LLP

Gail E Crawford gail.crawford@lw.com
Fiona M. Maclean fiona.maclean@lw.com

Latham & Watkins LLP