KEMP IT LAW

Tech Law at the Apex

White Paper

Legal Aspects of Artificial Intelligence (v. 4.0)

Chris Kemp, December 2022

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE
TABLE OF CONTENTS

TABLE OF FIGURES, TABLES AND ANNEXES

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE (v. 4.0)[1]

A. INTRODUCTION

1. **The pace of change.** Moore's law – the observation that the number of transistors that can be squeezed onto a computer chip doubles every two years – has long been a byword for the pace of change in computer technology. But Moore's law does not capture the current pace of change in artificial intelligence ("**AI**").

   Take the number of parameters in the most advanced AI models as an example. Parameters are coefficients applied to the calculations carried out by an AI model. The number of parameters is a rough proxy for an AI model's complexity. In 2018, Google's BERT language model was considered state of the art with 100 million parameters. In 2022, the most advanced AI models contained over 1 trillion parameters. The specifications of supercomputers currently under development suggests AI model sizes will reach half a quadrillion parameters in the coming years.[2] The economic costs of training these vast AI models is also staggering. Some suggest that by the middle of the decade it could cost US$ 1 billion to train a cutting-edge AI model.[3]

   The blistering pace of change means that AI is emerging as the key driver of the 'fourth industrial revolution' the term (after steam, electricity and computing) coined by Davos founder Klaus Schwab for the deep digital transformation now under way.[4]

2. **What is AI?** In 1950, Alan Turing proposed what has become known as the Turing Test for calling a machine intelligent: a machine could be said to think if a human interlocutor could not tell it apart from another human.[5] Modern definitions of AI vary. In its 2018 book *The Future Computed*, Microsoft thinks of AI as:

   > *a set of technologies that enable computers to perceive, learn, reason and assist in decision-making to solve problems in ways that are similar to what people do*.[6]

   In the language of technical standards, the International Organization for Standardization ("**ISO**") defines AI as an:

   > *Interdisciplinary field… dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning.*[7]

   The Organization for Economic Co-operation and Development ("**OECD**"), in an approach which has influenced the European Union's thinking on AI regulation, defines an 'AI system' as:

   > *a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.*[8]

---

[1] The main changes to this version are: (1) adding a new case study on 'AI as a Service' (AIaaS) (C.14 to C.16); (2) updating the Connected and Autonomous Vehicles (CAVs) case study, in light of the conclusion of the Law Commissions automated vehicles report (C.19 and C.20); and (3) updates to AI regulation section, mainly in light of recent EU developments (E.29 to E.34).

[2] 'Huge "foundation models" are turbo-charging AI progress', *The Economist*, 11 June 2022 <https://tinyurl.com/2p86mjk8>.

[3] Nicole Hemsoth, 'The billion dollar AI problem that just keeps scaling', *www.nextplatform.com,* 11 February 2021 <https://tinyurl.com/2jpppssn>.

[4] Klaus Schwab, *The Fourth Industrial revolution* (World Economic Forum, 2016).

[5] Alan Turing, 'Computing Machinery and Intelligence', *Mind*, 1 October 1950 <https://tinyurl.com/4nm3x944>.

[6] Microsoft Corporation, *The Future Computed: Artificial Intelligence and its Role in Society*, 2018 <https://tinyurl.com/3x3z96rw>.

[7] ISO/IEC 2392:2015, definition 2123769 <https://tinyurl.com/4wanbsuu>. (ISO/IEC 2392:2015 is the ISO/IEC's core IT vocabulary standard.)

[8] OECD, *Recommendation of the Council on Artificial Intelligence,* OECD/LEGAL/0449, 22 May 2019 <https://tinyurl.com/a5ffu35m>.

3. **The technical context.** Since the early years of AI in the 1950s, AI has progressed unevenly. Some researchers have identified three distinct eras in the development of AI. First, the 'pre-deep learning' era running from the early 1950s to 2010, when the computer processing power (often called 'compute') required to power AI models doubled roughly every two years (i.e. in step with Moore's law). Second, the ongoing 'deep learning' era, which began in 2010 and where compute requirements grew rapidly (doubling every six months) thanks in large part to the developments in graphics processing unit ("**GPU**") technology. Third, the 'large-scale model' era which, beginning in 2015, is characterised by the development and release of extremely large AI models by leading tech companies – BERT being a good example (A.1 above).[9]

   These developments have led to the emergence of several separate, related AI technology streams – machine learning, natural language processing ("**NLP**"), expert systems, vision, speech, planning and robotics (see Section B below). Although much processing takes place between machines, it is in interacting with people that AI particularly resonates, as NLP starts to replace other interfaces and AI algorithms 'learn' how to recognise images ('see') and sounds ('hear' and 'listen'), understand their meaning ('comprehend'), communicate ('speak') and infer sense from context ('reason').

4. **The business context.** Many businesses that have not previously used AI proactively in their operations will start doing so in the coming months and years. Market research company IDC predicts that global spending on AI will nearly triple from $118 billion in 2022 to $300 billion in 2026. This would amount to a compound annual growth rate ("**CAGR**") in the sector of 26.5% over the period. To put this in context, this is over four times greater than the predicted CAGR for global IT spending generally over the same period (6.3%). Sectors with the highest spend on AI are forecast to be banking, retail, professional services and manufacturing. The four greatest AI use cases are expected to be: augmented customer service agents; sales process recommendation and augmentation; fraud analysis and investigation; and program advisors and recommendation systems. Together, these areas are projected to represent more than 38% of global AI spending.[10]

5. **The legal, policy and regulatory context.** The start point of the legal analysis is the application to AI of developing legal norms around software and data. Here, "it's only AI when you don't know how it works, then it's just software and data" is a useful heuristic. In legal terms, AI is a combination of software and data. The software (instructions to the computer's processor) is the implementation in code of the AI algorithm (a set of rules to solve a problem). What distinguishes AI from traditional software development is, first, that the algorithm's rules and software implementation may themselves be dynamic and change as the machine learns; and second, the very large datasets that the AI processes (as what was originally called 'big data'). The data is the input training, testing and operational datasets; that input data as processed by the computer; the output data from those processing operations; and data derived from the output data.

   In policy terms, the scale and societal impact of AI distinguish it from earlier generations of software. This is leading governments, industry players, research institutions and other stakeholders to articulate principles (around fairness, safety, reliability, privacy, security, inclusiveness, accountability and

[9] Jaime Sevilla et al, *Compute Trends Across Three Eras of Machine Learning*, 9 March 2022 <https://tinyurl.com/27w5h2f3>. See also Neil C. Thompson et al, *The Computational Limits of Deep Learning*, 27 July 2022 <https://tinyurl.com/233k3nzs>.

[10] IDC, *Worldwide Spending on AI-Centric Systems Will Pass $300 Billion by 2026, According to IDC*, 12 September 2022 <https://tinyurl.com/kcez39tf>.

transparency) and policies that they intend to apply to all their AI activities. As the rate of AI adoption increases, general legal and regulatory norms – in areas of law like intellectual property, data protection and negligence – and sector specific regulation – in areas like healthcare, transport and financial services – will evolve to meet the new realities.

6. **Scope and aims of this white paper.** This white paper is written from the perspective of the in-house lawyer working on the legal aspects of their organisation's adoption and use of AI. It:

   - overviews at Section B the elements and technologies of AI;
   - provides at Section C three case studies that look at technology and market developments in greater depth to give more practical context for the types of legal and regulatory issues that arise and how they may be successfully addressed. The case studies are (1) 'AI as a Service' (AIaaS) (C.14 to C.16) legal services (C.17 and C.18) and connected and autonomous vehicles (C.19 and C.20);
   - reviews at Section D the legal aspects of AI from the standpoints of intellectual property law (D.23 and D.24), data protection (D.25), agency law (D.26), contract law (D.27) and tort law (D.28);
   - considers at Section E regulatory and policy development across three jurisdictions: the EU (E.30 to E.32), the US (E.33) and the UK (E.34); and
   - considers at Section F ethics and governance of AI in the organisation.

   The Annex is a short glossary of terms used. This white paper is general in nature and not legal advice. It is written as at 6 December 2022 and from the perspective of English law.

B. THE TECHNOLOGIES AND STREAMS OF AI

7. **The cloud and AI as twinned convergences: importance of the cloud.** Developments in AI have been fuelled by the ability to harness huge tides of digital data. The vast volumes of varied data arriving at velocity are a product of the cloud, shown in Figure 1 below as the convergence of data centres, the internet, mobile and social media. Data centres – increasingly in the form of huge 'hyperscale' sites[11] – are the engine room of the cloud. Billion-dollar investments in millions of square feet of space housing over a million servers will support more than a quadrupling of the size of the global cloud computing industry to c.$1.5 trillion in the eight years to 2030.[12]

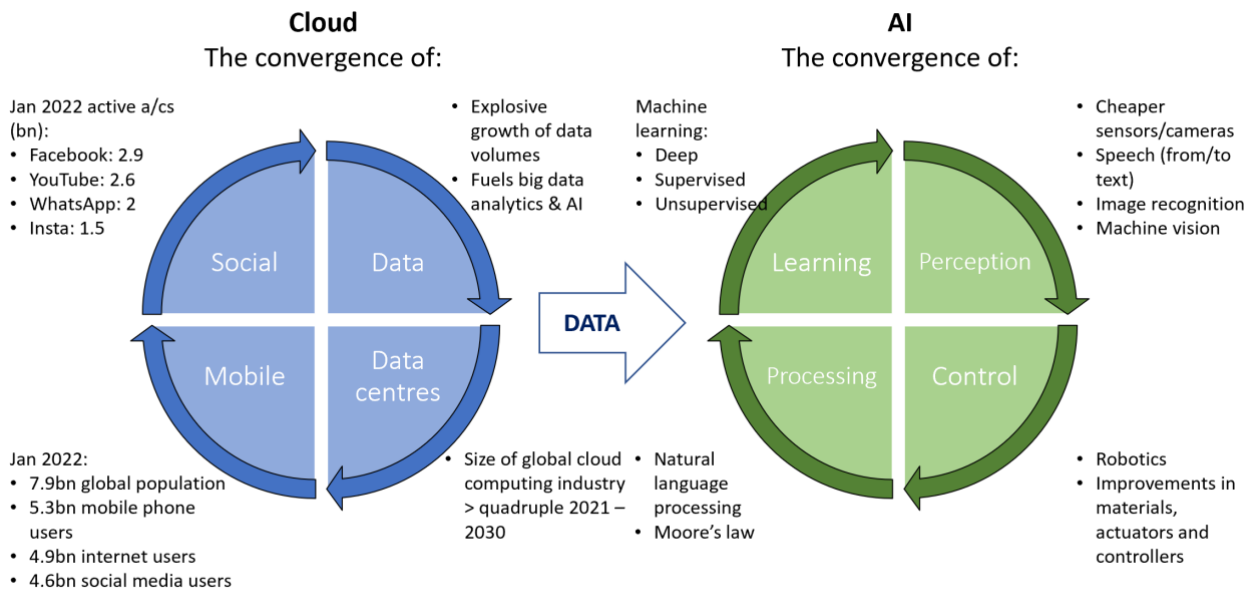
   Internet, mobile, video streaming and social media use at scale are in turn driving the cloud. For a global population of over 8 billion in Q4 2022, there are estimated to be more than 5.3 billion unique mobile phone users, 4.9 billion internet users and 4.6 billion active social media users. Increasing internet, mobile and social media use is in turn continuing to fuel an explosion in digital data volumes. In H1 2021, video streaming and social media accounted for 66% of overall internet traffic, with YouTube alone accounting for c.15%. Every minute of the day, TikTok users watch 167 million videos, Netflix users stream 684

[11] Generally understood to mean a data centre housing a minimum of 5,000 servers and at least 10,000 square feet in size, though given the pace of change 'hyperscale' is as well understood to be a marketing term as a classification type. The largest operators (Google, Microsoft, Amazon Web Services, etc.) are increasingly referred to as operating at 'mega hyperscale'.

[12] Cision PR Newswire, *www.prnewswire.com*, 'Cloud Computing Market Size Worth $1,554.94 Billion by 2030: Grand View Research, Inc.', 24 February 2022 <https://tinyurl.com/2n4jbdx4>.

thousand hours of video content, and Zoom hosts 856 minutes of webinars.[13] It is the availability of data at this scale that provides the raw materials for AI.

Figure 1: Twinned convergences: the cloud and AI



8. **AI: convergence, technologies and streams.** On the other side of these twinned convergences AI can be represented as the convergence of different types of machine capability and the different technologies or streams of AI.

AI can be seen (see Figure 1 above) as the convergence of four areas of machine capability – processing (B.9 below), learning (B.10), perception (B.11) and control (B.12). In the words of Jerry Kaplan in *Humans Need not Apply*, what has made AI possible is:

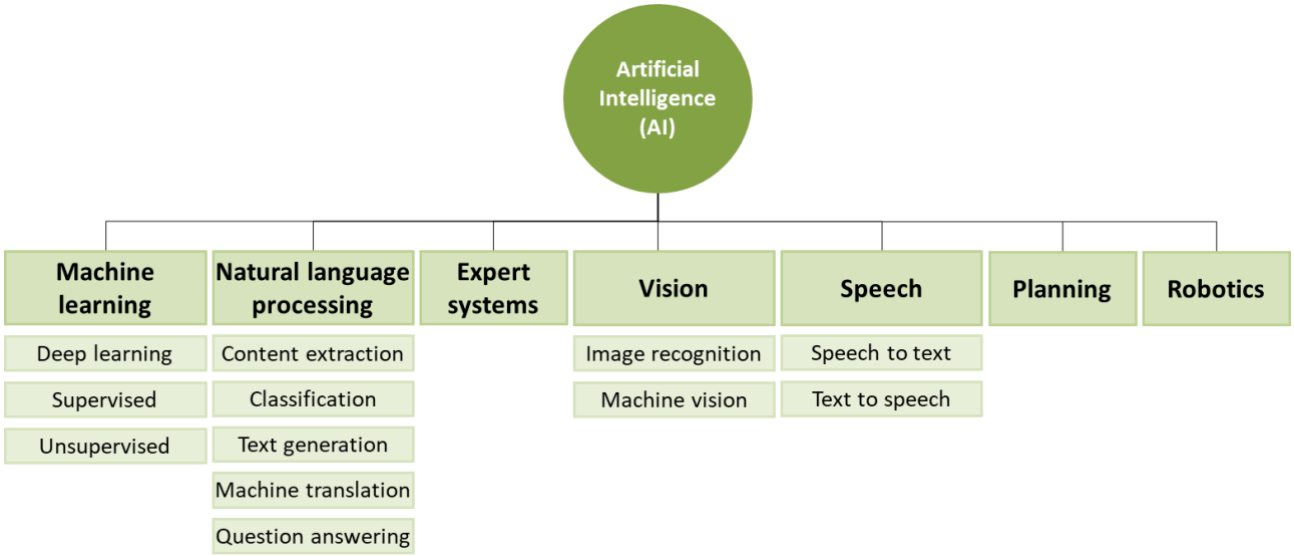
> *the confluence of four advancing technologies… vast increases in computing power and progress in machine learning techniques… breakthroughs in the field of machine perception… [and] improvements in the industrial design of robots.*[14]

AI is a set of technologies not a single one and can also be seen as a number of streams, as shown in Figure 2 below. The main streams are machine learning and NLP, expert systems, vision, speech, planning and robotics. This section maps these streams to the four main areas of machine capability.

[13] Sources: (i) global population: *Worldometers.info* <https://tinyurl.com/2p8nhxb5>; (ii) mobile, internet and social media users: *Datareportal.com*, 'Digital 2022: Global Overview Report', 26 January 2022 <https://tinyurl.com/2w7p4bwb>; (iii) video streaming and social as percentage of internet traffic: Sandvine, 'The Global Internet Phenomena Report January 2022' <https://tinyurl.com/48hvut33>; and (iv) TikTok, Netflix and Zoom: Domo, 'Data Never Sleeps 9.0', October 2021 <https://tinyurl.com/mty6ku9s>.

[14] Jerry Kaplan, *Humans Need Not Apply: A Guide to Wealth and Work in the Age of Artificial Intelligence* (New Haven and London: Yale University Press, 2015), pp. 38-39.

Figure 2: The main AI streams



9. **Machine processing: Moore's law and GPUs.** In 1965 Intel co-founder Gordon Moore famously predicted that the density of transistors (microprocessors) on an integrated circuit (chip) would double approximately every two years. This rule held good for fifty years as computer processor speeds reliably doubled every 18 to 24 months. Although Moore's law is running out of steam as processor density increasingly produces counter-productive side-effects like excess heat, it remains a fundamental driver of the computer industry for now.[15]

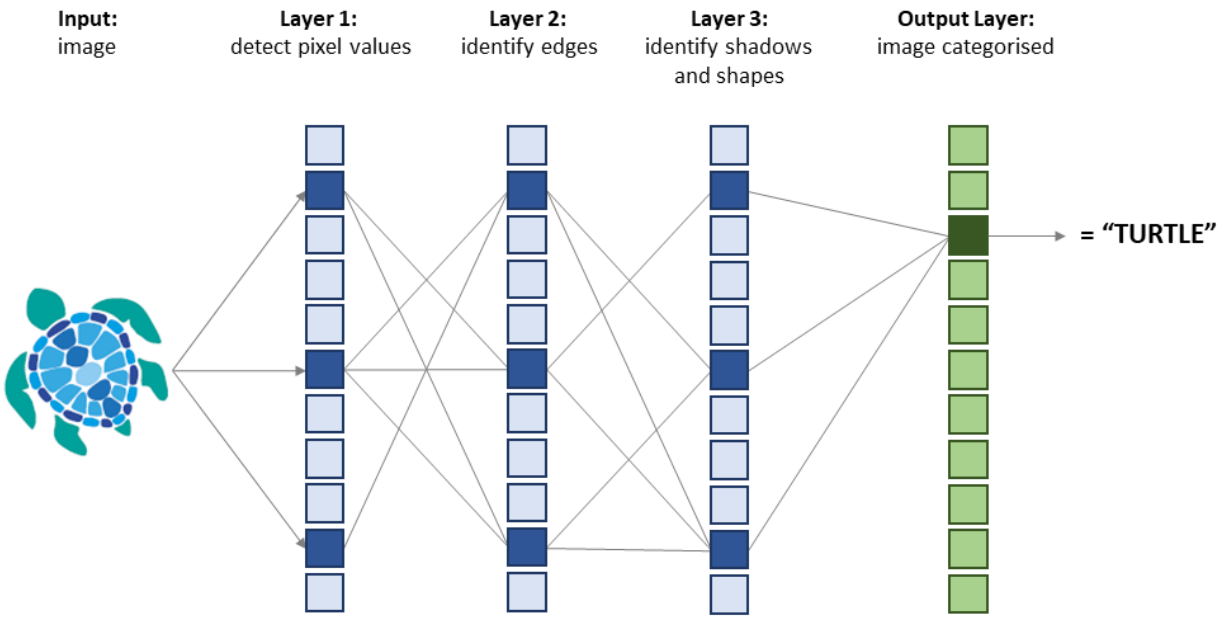
   What has also particularly sped up the development of AI was the realisation from about 2010 that GPUs (processors that perform computational tasks in parallel) originally used for videos and gaming as adjuncts to computers' central processing units ("**CPUs**", processors that perform computational tasks in series) were well suited to the complex maths of AI.

10. **Machine learning: modalities – deep, supervised and unsupervised.** Exponential growth in computer processing power has enabled the development of the streams of machine learning – deep learning, supervised learning and unsupervised learning – by which computers learn by example or being set goals and then teach themselves to recognise patterns or reach the goal without being explicitly programmed to do so.

    Deep learning. Deep learning uses large training datasets to teach AI algorithm software implementations to accurately recognise patterns and other input data in what are called artificial neural networks. Artificial neural networks, which consist of a network of simple information processing units known as 'nodes' or 'neurons', are inspired by the structure of the human brain.[16] A simplified diagram of an artificial neural network is shown in Figure 3 below: in the diagram a computer teaches itself to identify an image of a turtle by first breaking down input data into groups of pixels and then into layers. Information analysing the problem is passed from layer to layer of increasing abstraction and then combined in stages until the final output layer can categorise the entire image.

[15] For more on the future of Moore's law, see Mark Radosavljevic et al in *IEEE Spectrum*, '3D-Stacked CMOS Takes Moore's Law to New Heights', 11 August 2022 <https://tinyurl.com/sudsv33m>.
[16] For an explanation which begins to explore the computational mathematics behind neural networks, see John D. Kelleher, *Deep Learning* (USA: The MIT Press, 2019), chapter 3.

Figure 3: Artificial neural networks[17]



Neural networks work in layers. (1) The computer's memory presents an input to the network – a pixelated image of a turtle. (2) Data from a pixel in the Input causes a neuron in Layer 1 (a square in the graphic) to signal its analysis to neurons in Layer 2, and so on. (3) Each layer analyses a particular aspect of the input, like edges, shadows and shapes. (4) The features are combined level by level until the Output Layer categorises the entire image.

Training a neural network to make accurate predictions involves calibrating the relationship, or 'weight', between two connected neurons. Once trained, fine tuning decreases the error rate and increases the accuracy of predictions.

Deep learning is emerging as AI's 'killer app' enabler, and this approach – using machine learning software to reduce prediction error through training and fine tuning before processing operational workloads – is at the core of many uses of AI. It is behind increasing competition in AI use in many business sectors including law (standardisable componentry of repeatable legal tasks), accountancy (auditing and tax), insurance (coupled with IoT sensors) and autonomous vehicles.

In ***supervised learning*** the AI algorithm is programmed to recognise a sound or image pattern and is then exposed to large datasets of different sounds or images that have been labelled so the algorithm can learn to tell them apart. For example, to recognise the image of a turtle, the algorithm is exposed to datasets labelled as turtles and tortoises so it can recognise one from the other.

Labelling is time-consuming and expensive, particularly when human experts are required to do it, so in ***unsupervised learning*** the data that the algorithm instructs the computer to process is not labelled; rather, the system is set a particular goal – to reach a high score in a game for example – and the AI is then exposed to large unlabelled datasets that it instructs the computer to process to find a way to reach the goal.

[17] Source: turtle graphic – House of Lords Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?*, HL Paper 100 (April 2018), p. 21 <https://tinyurl.com/4amp7b93>.

11. **Machine perception: NLP, expert systems, vision and speech.** Machine learning techniques when combined with increasingly powerful and inexpensive cameras and other sensors are accelerating machine perception – the ability of AI systems to recognise, analyse and respond to the data around them (whether as image, sound, text, unstructured data or in combination) and 'see', 'hear', 'listen', 'comprehend', 'speak', and 'reason'.

    Driven by recent breakthroughs in 'transformer' or 'foundational' AI models,[18] ***NLP*** is emerging as a primary user interface for AI systems and will in time replace the graphical user interface ("**GUI**") just as the GUI replaced the command line interface ("**CLI**"). Enabled by increasing accuracy in voice recognition, systems can respond to one-way user input requests and are now interacting in two-way conversations. A poignant recent development has been the ability of leading transformer NLP models to analyse and explain jokes, with Google's 2022 PaLM model being a good example.[19]

    Expert systems look to emulate human decision-making skills by applying rules (known as the 'inference engine') to the facts and rules in the system (its 'knowledge base'). Thomson Reuters' Data Privacy Advisor, launched in January 2018 and the first application to market in the Watson collaboration between IBM and Thomson Reuters, is a good example.

    Vision is currently the most prominent form of machine perception, with applications using deep neural networks to train AI systems to recognise faces, objects and activity. Striking recent developments have been made in the realms of 'text to image' (where an AI model produces an image from some input text) and 'text to video' (the same, but the model produces a video). For example, Figure 4 below is an image produced by AI research company OpenAI's Dall·E model when given the text prompt "A picture of a rabbit in the style of Hans Holbein the Younger's portrait of Henry VIII".[20] Leading recent examples of 'text to video' developments are Meta's Make-A-Video[21] and Google's Imagen Video.[22]

    Machine perception is also developing quickly in ***speech***, where accuracy has met or exceeded that of professional human transcribers for some years now.[23] A notable trend here is the burgeoning world of text-to-speech ("**TTS**") audio generation services – where, for example, a written newspaper article is converted into an audio file 'spoken' in the 'voice' of the journalist.[24]

[18] 'Artificial intelligence's new frontier', *The Economist*, 9 June 2022 <https://tinyurl.com/2ytha83c>.
[19] Janus Rose, 'Google Is Teaching AI to Explain Your Jokes to You', *Vice*, 11 April 2022 <https://tinyurl.com/3j2ksmxu>.
[20] At the time of writing, OpenAI's Dall·E image generation model is free to use, and well worth exploring: <https://tinyurl.com/4pee4re3>.
[21] Meta, *makeavideo.studio* <https://tinyurl.com/5c2vr9pm>.
[22] Google, *imagen.research.google* <*https://tinyurl.com/yj72p8xt*>.
[23] Since August 2017 in Microsoft's case: see Microsoft Blog, 'Microsoft researchers achieve new conversational speech recognition milestone' (20 August 2017) <https://tinyurl.com/2s3dsann>.
[24] See for example the work of market-leading TTS platform BeyondWords <https://tinyurl.com/bdfxbarv>.

Figure 4: Image generated by OpenAI's Dall·E model

An image generated by OpenAI's Dall·E model using the text prompt: "A picture of a rabbit in the style of Hans Holbein the Younger's portrait of Henry VIII".

12. **Machine control: robotics and planning.** Machine control is the design of robots and other automated machines using better, lighter materials and better control mechanisms to enhance the speed and sensitivity of machine response in 'sensing → planning → acting'. Machine control adds to the combination of machine learning and machine perception in a static environment the facility of movement in and manipulation of an interactive environment. Essentially, mobile AI is more challenging than static AI and machine control will build on developments in machine learning (particularly reinforcement learning) and perception (particularly force and tactile perception and computer vision).

    These developments are seen in the rapid global growth in industrial robotics, which has rebounded strongly since the COVID-19 pandemic. According to the International Federation of Robotics, an industry group, over half a million new industrial robots were installed worldwide in 2021, an all time high. Chinese demand is particularly strong in this area, with China installing more industrial robots in 2021 than the rest of the world taken together.[25]

C. AI IN PRACTICE: CASE STUDIES

13. **Introduction.** Whilst AI can be broken down into its constituent technologies and streams irrespective of particular use cases, examining the practical application of AI to particular industry sectors will assist in providing a context for reviewing the legal aspects of an organisation's AI projects. Accordingly this section

[25] International Federation of Robotics, World Robotics 2022 slide deck, 13 October 2022 <https://tinyurl.com/3p9d5zcr>.

works through three case studies, highlighting in each case background market and technology developments and then reviewing legal and regulatory aspects.

Case Study 1: AI as a Service ("AIaaS")

14. **AIaaS: the technical & business context.**

The AIaaS platform ecosystem. For all its technical novelty, AI is no exception to the trend for rapid commoditisation in cloud services. The big cloud vendors (Amazon Web Services ("**AWS**"), Microsoft (via the Azure cloud platform) and Google (via Google Cloud Platform ("**GCP**") among a handful of others) offer an expanding range of standardised, pre-configured AI-enabled services. For example, services which enable app or website owners to deploy chatbots; financial services and insurance companies to detect online fraud; and research scientists to derive insights from unstructured medical data.[26]

Complementary trend: Services-Oriented Architecture ("SOA") and microservices. The decline in popularity of monolithic software architectures and the emergence of SOA and microservices is a complementary trend, which has also stimulated the adoption of cloud services like AIaaS. In monolithic software architectures, an application is built and deployed as a single unit. By contrast, SOA and microservices offer software applications composed from small, discrete units of functionality – for instance, a text translation tool or an image recognition function. For software vendor Red Hat, SOA and microservices are "widely considered to be one of the building blocks for a modern IT infrastructure"; their rise makes it cheaper and easier to build, integrate and deploy AIaaS functionality within a larger application.[27]

Advantages of commoditised AI services. The commoditisation of AI functionality in AIaaS can offer businesses significant advantages:

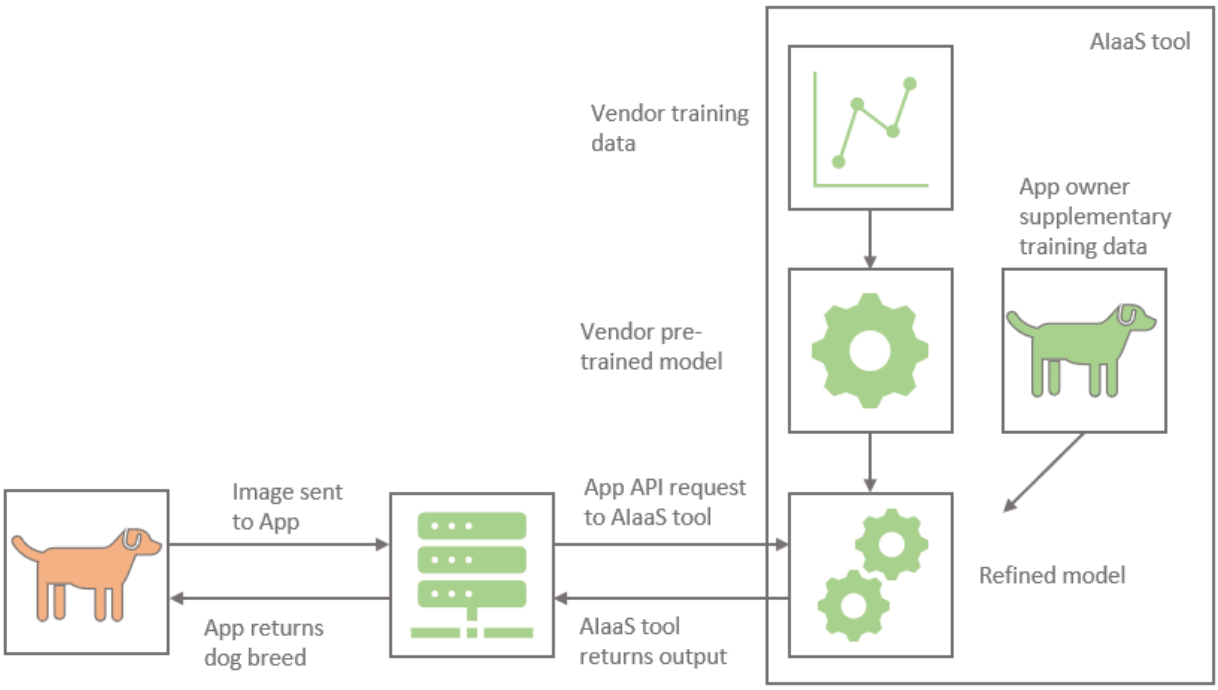
- avoid the upfront capital cost of IT infrastructure required to deploy AI and ongoing maintenance;
- 'pay as you go' model helps avoid inefficiencies in underutilised hardware/software investments;
- avoid need to train up or hire specialist personnel;
- pre-trained AI models can be used 'out of the box' or with minimal additional training or configuration; and
- ease of integration with other elements of a business's cloud-hosted IT stack.

15. **AIaaS: simple introductory example.**

Example: image recognition app that uses AIaaS. Figure 5 below shows, as a simplified example, a mobile app that enables a user to identify a breed of dog by taking a photo in the app. The app uses a cloud-based AIaaS image recognition tool.

[26] See, for example: AWS, 'Machine Learning on AWS' <https://tinyurl.com/27p87v2n>; Azure, 'Azure Cognitive Services: Deploy high-quality AI models as APIs' <https://tinyurl.com/2zpd4zuy>; and GCP, 'AI and Machine Learning <https://tinyurl.com/2bk4kjem>.
[27] Red Hat, '6 overlooked facts of microservices', 4 February 2021 <https://tinyurl.com/3ajp7yf8>.

Figure 5: An app uses an AIaaS image recognition tool to identify dog breeds



In the example in Figure 5, the end user takes a photo of a dog using the app on a mobile device. The app then submits the image to a cloud-based AIaaS tool for analysis via an API request.[28] The image is then processed by a model which has been specifically calibrated to recognise different breeds of dog (the "refined model").

The app developer has taken advantage of the tools within the cloud-based AIaaS platform it uses to develop the refined model quickly and cheaply, instead of starting from scratch. The app developer began by using a pre-trained image recognition model 'off the shelf' in the AIaaS platform. The pre-trained model had been trained on generic public datasets:[29] it worked well as a generic image recognition tool, but lacked sufficient dog breed data to operate effectively as a dog breed classification tool. The app developer decides to fine-tune the pre-trained model with supplementary training data – in this case the app developer's proprietary database, consisting of several thousand images of dogs, each labelled according to the specific breed. Having been trained on this supplementary data, the refined model can determine the dog breed in a given input image with a satisfactory degree of accuracy and reliability.

This method of fine-tuning a generic model using specialist data is known as 'transfer learning' and can be distinguished from both 'full training', where a model is initialised with random weights (see B.10 above) and trained entirely on the app developer's data, and using a model 'off the shelf', where the pre-trained model is used with no additional training data.[30]

[28] An API is a set of standardised rules that allows data to be communicated between different pieces of software. In this case, the app and the AIaaS tool.
[29] With a common example being ImageNet <https://tinyurl.com/bddwuttw>, an influential image database containing around 14m images at the time of writing.
[30] See further Amazon Web Services, Amazon SageMaker: Developer Guide, <https://tinyurl.com/37yavf64> 'Image Classification Algorithm', pp. 2059 – 2062.

The example in Figure 5 is an oversimplification and, depending on the app architecture choices the app developer makes, the app can be structured in many ways. For instance, more or less of the app could be deployed in the cloud. Additional microservices could be bolted on to the app to add extra functionality as the platform grows: e-commerce functionality (pet food, pet accessories, etc.) or social media integrations could be added, for instance. In this way, the AIaaS element of an app would form part of a larger whole.

16. **AIaaS: legal issues.**

Cloud vendor's standard terms. Consistent with the commoditised nature of AIaaS, customers using popular cloud-based AIaaS platforms may not be able to negotiate commercial and legal terms with the vendor, except for the most significant projects – either in terms of the value of the deal or its novelty or strategic importance for the vendor. If this is the case, the operational risk the customer takes on can often be underappreciated. Whether a customer's entire application or business system is hosted by a third-party cloud vendor, or only a small but important part of it, unfavourable terms (e.g. a right for the vendor to terminate for convenience) could lead to significant business disruption for the customer. If it is not possible to negotiate terms, the customer could look to mitigate risk operationally – e.g. estimating time and cost required to implement a system with an alternative vendor.

AIaaS and privacy issues. As with cloud services generally, cloud-hosted AIaaS has been affected by the fallout form the CJEU's 2020 'Schrems II' decision. The issues surrounding international transfers of personal data in AIaaS are much the same as for other areas of cloud computing with an international transfers element.[31] In AIaaS, however, the privacy risks are exacerbated by stricter rules that apply to automated decision-making in the GDPR (in both its UK and EU flavours). Where an AIaaS processes personal data, additional disclosures may be required in privacy policies. By Art. 13(2)(f) of UK/EU GDPR, this would include "meaningful information about the logic involved" in the AIaaS. However, because the customer has outsourced core AI aspects to the AIaaS vendor, the required information may not be readily available. The risks associated with this rather convoluted compliance position are increased if the AIaaS vendor asks (as they often do) that the customer give a contractual commitment to provide all necessary privacy information to the relevant data subjects. The implications of the general prohibition on automated individual decision-making in Art. 22 UK/EU GDPR are considered in more detail at D.25 below.

Automated fairness and bias mitigation tools. The big cloud vendors now offer pre-packaged tools as part of their AIaaS offerings which aim to help users improve fairness and mitigate bias in AI modelling. One example is Microsoft Azure's Fairlearn product.[32] Fairlearn is a suite of tools which *assess* fairness-related metrics in AI models and a range of algorithms which can help *mitigate* unfairness in AI models. Similarly AWS's SageMaker Clarify product aims to help users identify potential bias both in pretraining data and when an AI model is used in production.[33] SageMaker Clarify "also provides tools to help you generate model governance reports that you can use to inform risk and compliance teams, and external regulators."[34]

While fairness toolkits such as these may serve as a useful starting point for addressing fairness and bias issues in the context of AIaaS, they are not (as the big cloud vendors generally make clear) a one-stop-

[31] For more on this, see Eleanor Hobson's recent blog: *International Transfers Summer 2022 update* <https://tinyurl.com/yxd6dbxx>.
[32] See here: <https://tinyurl.com/2we34hse>.
[33] See here: <https://tinyurl.com/nssuuzx9>.
[34] Amazon Web Services, *Amazon SageMaker: Developer Guide*, <https://tinyurl.com/37yavf64> 'Image Classification Algorithm', p.7.

shop for compliance. Microsoft notes in a 2020 white paper on Fairlearn and fairness in AI that "prioritizing fairness in AI systems is a sociotechnical challenge. Because there are many complex source of unfairness… it is not possible to fully "debias" a system or to guarantee fairness".[35] Similarly, AWS states that "the output provided by Amazon SageMaker Clarify is not determinative of the existence or absence of statistical bias".[36]

Case Study 2: AI in legal services

17. **AI in legal services: market developments.**

Background: AI and the legal services market. The legal services sector is a £42bn industry in the UK accounting for around 2% of GDP. It is representative of UK professional services generally, which accounts for £194bn or 10% of UK GDP.[37]

IT in legal services began in the 1970s with information retrieval, word processing and time recording and billing systems. The 1980s saw the arrival of the PC, office productivity software and the first expert systems; and the 1990s, email, practice and document management systems. In the 2000s Google grew to "become the indispensable tool of practitioners searching for materials, if not solutions". There has been further progress in recent years around contract diligence, e-discovery and legal project management.[38] There has been further progress in recent years around contract diligence, e-discovery and legal project management. The 2020s are predicted to be the decade of AI systems in the professions.[39]

Over this fifty-year period the number of UK private practice solicitors has grown almost five times, from just under 20,000 in 1968 to 97,000 in 2021. The rate of growth of UK in-house solicitors is even more dramatic, increasing by eighteen times from 2,000 in 1990 to around 36,000 in 2021. The ratio of in-house to private practice solicitors in the UK now stands at around 1:3, up from 1:2 in 1990.[40]

These long-term developments in IT use and lawyer demographics are combining with recent rapid progress in AI, the legacy legal and regulatory complexity of business since the 2008 financial crisis and the realities of working life in the wake of the COVID-19 pandemic to drive change in client requirements at greater scale and speed than previously experienced towards greater efficiencies, higher productivity and lower costs.

How will AI drive change in the delivery of legal services? Much of the general AI-driven change that we are all experiencing applies to lawyers and is here today – voice recognition and NLP (speaking into the device), digital personal assistants (organising the day), augmented reality (learning and training) and instantaneous translation (Bing and Google Translate).

---

[35] Microsoft et al., *Fairlearn: A toolkit for assessing and improving fairness in AI* (22 September 2020) <https://tinyurl.com/5n6shat6>.
[36] AWS Service Terms <https://tinyurl.com/ycxdx8m3> (version dated 2 December 2022) Section 60.5.
[37] £42bn: Office for National Statistics, *Turnover of legal activities*, January 2020 to March 2022 (year to March 2022) <https://tinyurl.com/bdfj62p9>. £194bn: TheCityUK, *Key facts about UK-based financial and related professional services 2021* <https://tinyurl.com/2p9ybbrh>, p.3.
[38] See further Orlando Conetta, 'AI in the Legal Profession' in *The Law of Artificial Intelligence*, ed. by Matt Hervey and Matthew Lavy (London: Sweet & Maxwell, 2021), pp.557-574.
[39] See further Richard and Daniel Susskind, *The Future of the Professions: How Technology will Transform the Work of Human Experts* (Oxford: OUP, 2022), p.206.
[40] The Law Society, *Trends in the Solicitors' Profession: Annual Statistics Report 2021* (21 September 2022) <https://tinyurl.com/5fmhmcr7>.

In consumer legal services (wills, personal injury, domestic conveyancing, etc.), AI and automation are intensifying competition and consolidation, reducing prices, and extending the market.

In business legal services, current AI use cases centre on repeatable, standardisable components of work areas like contract automation, compliance, litigation discovery, due diligence in M&A and finance and property title reports.

What might AI in business legal services look like at scale? A number of pointers:

- competition will drive adoption – clients will want their law firm to have the best AI;
- cloud-based AI as a Service ("**AIaaS**") will become a commodity, giving legal services providers complex "make/buy" choices (between developing their own technology and buying it in);
- law firms may not be the natural home for legal AI at scale and other providers (like the Big 4 accounting firms, legal process outsourcers ("**LPOs**"), integrators and pure play technology providers) may be more suited to this type of work in the long run;
- smart "**APIs**" (application programming interfaces) will give General Counsel more choice and control over output and cost by enabling different parts of the service to be aggregated from different providers – in-house, law firm, LPO and AI provider – and then seamlessly combined. In M&A for example, having the AI analyse and report on a larger proportion of the target's contract base may reduce diligence costs (typically 20% to 40% of the acquirer's law firm's fees) and allow more time for higher value work; and
- network effects will lead to consolidation as the preference develops to "use the systems that everyone uses".

18. **AI in legal services: regulatory and legal aspects.**

Background: regulatory structure for legal services in England and Wales. The regulatory structure for legal services here came into effect in October 2011 when most of the Legal Services Act 2007 ("**LSA**") came into force. It follows the normal UK pattern of making the provision of certain types of covered services – called "reserved legal activity" in the LSA – a criminal offence unless the person supplying them is authorised (s.14, LSA). "Reserved legal activity" is defined at s.12(1) and Schedule 2 LSA and is a short list[41] so that most "legal activities"[42] are unregulated.[43] The Legal Services Board ("**LSB**") oversees the

[41] Essentially, (i) court audience rights; (ii) court conduct of litigation; (iii) preparing instruments transferring land or interests in it; (iv) probate activities; (v) notarial activities; and (vi) administration of oaths.
[42] Defined at s. 12(3) LSA as covering: (i) reserved legal activities; and (ii) otherwise in relation to the application of law or resolution of legal disputes, the provision of (a) legal advice and assistance or (b) legal representation.
[43] Contrast the position in the USA for example, where the US State Bar Associations much more zealously protect against the unauthorised practice of law.

regulation of lawyers and has appointed eight approved regulators, of which the Solicitors Regulation Authority ("**SRA**") is the primary regulator of solicitors.[44]

Indirect regulation. In addition to direct regulation, law firms and other legal services providers ("**LSPs**") may be indirectly regulated by their clients' regulator where that client is itself regulated, for example by the Financial Conduct Authority ("**FCA**") or the Prudential Regulation Authority ("**PRA**"). This indirect regulation arises through the client regulator's requirements as they apply to the client's contractors and supply chain, which would include its law firms, and the engagement contracts between the client and the law firm, which may flow down contractually certain of the client's regulatory responsibilities and requirements.

SRA Standards and Regulations. The regulatory standards and requirements that the "SRA… expect[s] [its] regulatory community to achieve and observe, for the benefit of the clients they serve and in the public interest" are contained in the SRA Standards and Regulations, which came into effect in November 2019.[45] At present, there are no regulatory requirements specifically applicable to AI and the relevant parts of the SRA Standards and Regulations are the same seven overarching Principles and parts of the SRA Codes of Conduct that apply generally.[46]

The Principles include acting: (i) in a way that upholds public trust and confidence in the solicitors' profession and in legal services; (ii) with independence, honesty and integrity; (iii) in a way that encourages equality, diversity and inclusion; and (iv) in the best interests of each client.

The SRA Standards and Regulations contain two codes of conduct: first, the Code of Conduct for Solicitors, registered European lawyers and registered foreign lawyers ("**SCCS**")[47] and second, the Code of Conduct for Firms ("**SCCF**").[48] Unlike the predecessor SRA Code of Conduct, the regime introduced in November 2019 is not prescriptive and does not contain explicit requirements about outsourcing. However, certain paragraphs of the SCCS and the SCCF will catch the use of AI services. For instance, SCCF paragraph 2.3 requires firms to "remain accountable for compliance with the SRA's regulatory arrangements where your work is carried out through others, including… those you… contract with." Likewise, SCCF 2.5 requires firms to "identify, monitor and manage all material risks to your business." Implicit in these paragraphs when a firm is using an AI service (whether third-party or proprietary) is an obligation to remain accountable and a requirement to take a risk-based approach.

[44] When the LSA came into force, the regulatory functions previously carried out by The Law Society of England and Wales were transferred to the SRA. The Law Society retains its representative functions as the professional association for solicitors. The other LSB approved regulators are: (i) the Bar Standards Board (barristers); (ii) CILEx Regulation (legal executives); (iii) the Council for Licensed Conveyancers; (iv) the Intellectual Property Regulation Board (patent and trademark attorneys) as the independent regulatory arm of the Chartered Institute of Patent Agents and the Institute of Trade Mark Attorneys; (v) the Costs Lawyer Standards Board; (vi) the Master of the Faculties (notaries); and (vii) the Institute of Chartered Accountants in England and Wales. In Scotland, solicitors have continued to be regulated by the Law Society of Scotland. The Legal Services (Scotland) Act 2010 in July 2012 introduced alternative providers of legal services as "licensed legal services providers". In Northern Ireland, regulatory and representative functions continue to be performed by the Law Society of Northern Ireland.
[45] Available at: <https://tinyurl.com/2p8h2jsh>.
[46] Available at: <https://tinyurl.com/yckam7sm>. The current version of the Principles has been in effect since November 2019 and were made by the SRA Board under (i) ss. 31 of the Solicitors Act 1974; (ii) s. 9 of the Administration of Justice Act 1985; and (iii) s. 83 of the LSA. Together with the SRA Codes of Conduct, they regulate the conduct of solicitors and their employees, registered European lawyers, recognised bodies and their managers and employees, and licensed bodies and their managers and employees.
[47] Available here: <https://tinyurl.com/rnks7jxb>.
[48] Available here: <https://tinyurl.com/4z449297>.

Client engagement terms: LSPs. LSPs using AI systems in client service delivery should consider using express terms around AI in their client engagement arrangements to set appropriate expectations for service levels and standards consistent with SRA duties. SRA-regulated LSPs, if seeking to limit liability above the minimum, must include the limitation in writing and draw it to the client's attention. Firms should therefore consider whether specific liability limitations for AI are to be included in their engagement arrangement terms.

Client engagement terms: clients. Equally, clients should insist that their law firms' engagement agreements appropriately document and expressly set out key contract terms around AI services. Clients operating in financial services and other regulated sectors will likely need to go further and ensure that their agreements with the law firms they use include terms that are appropriate and consistent with their own regulatory obligations around: (i) security relating to employees, locations, networks, systems, data and records: (ii) audit rights; (iii) continuity; (iv) exit assistance; and (v) subcontractors.

PII arrangements. As legal AI starts to proliferate, it is to be expected that in accepting cover and setting terms and premiums insurers will take a keener interest in how their insured law firms are managing service standards, continuity and other relevant AI-related risks.

Case Study 3: connected and autonomous vehicles ("CAVs")

19. **CAVs: market and technology aspects**

The CAV market. The projected growth rate of the global CAV market over the coming decade is striking on any measure. The UK Government transport and CAV innovation agency Connected Places Catapult estimates that the global CAV market will be worth £17bn by 2025. Connected Places Catapult's base projection is that this will rise to £650bn by 2035, a thirty eightfold increase, of which the UK CAV market will represent 6.4% (or £41.7bn). It is predicted that the vast majority of CAVs sold in 2035 will be cars (76%), followed by vans (20%) and then HGVs and buses (3%). CAV development is expected to have a profound impact in the long run on the structure of the global automotive industry and on global patterns of vehicle ownership and use.[49]

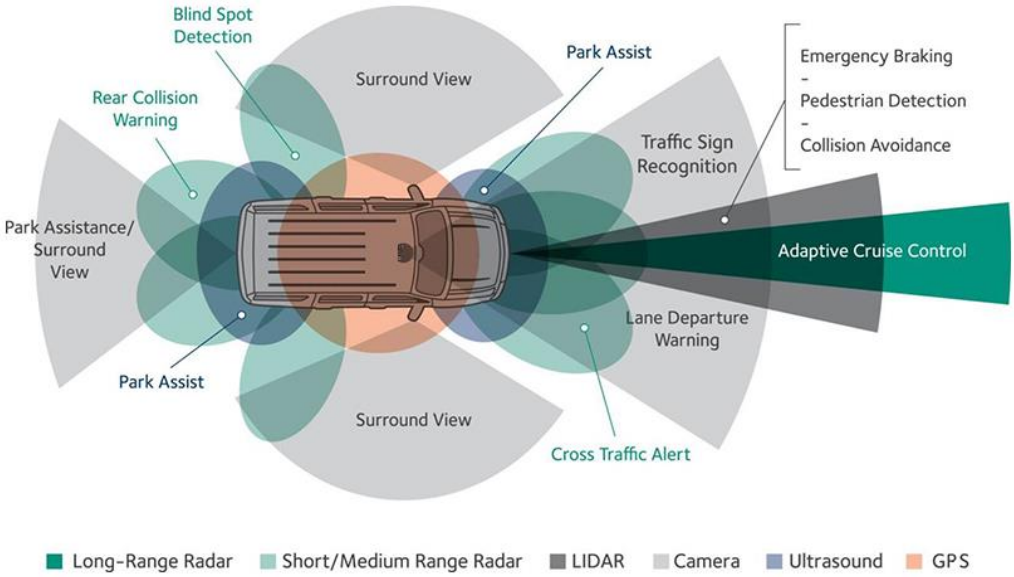
"Vehicles", "connectedness" and "autonomy". By "vehicles" we mean passenger cars and commercial vehicles, although AI of course will affect other types of vehicles as well as rail, sea, air and space transportation. "**Connected**" means that the vehicle is connected to the outside world, generally through the internet – most new cars sold today are more or less connected through services like navigation, infotainment and safety, often by means of a mobile phone. A threshold for "**autonomy**" is set in Section 1 of the UK's Automated and Electric Vehicles Act 2018 ("**AEVA**"). In the AEVA, a vehicle is autonomous (or "self-driving", in the words of the Act) if it is "designed or adapted to be capable, at least in some circumstances or situations, of safely driving itself". The distinction between autonomous/self-driving and mere "driver assistance" is a foundational concept in the emerging regulatory framework for CAVs.

Sensors, digital maps and the central computer. To act autonomously in this way, the CAV must constantly assess where it is located, the environment and other users around it, and where to move next. These assessments are made and co-ordinated constantly in real time by means of sensors, digital maps and a central computer. Figure 6 below shows the types of onboard sensors that a CAV uses to gather

[49] All figures from Connected Places Catapult, *Market Forecast for Connected and Autonomous Vehicles* (January 2021) <https://tinyurl.com/y6cfzbfd>.

information about its environment, including short, medium and long-range radar (**ra**dio **d**etection **a**nd **r**anging) and lidar (**li**ght **d**etection **a**nd **r**anging – essentially laser-based radar to build 3D maps), cameras and ultrasound.

Figure 6: CAVs' on board sensors[50]



In addition to sensors, autonomous vehicles rely on onboard GPS (global positioning system) transceivers and detailed pre-built digital maps consisting of images of street locations annotated with detailed driving feature information like traffic lights, signs and lane markings. These digital maps are increasingly updated in real time.

Sense → plan → act. The computer's system then receives the data from the sensors, combines it with the map and, using machine learning in a sequential 'sense → plan → act' three-step process, constantly (in effect, many thousands of time each second) determines whether, and if so where, when and how, to move. In the ***sensing*** phase, the computer uses the sensors to collect information. In the ***planning*** phase, it creates a digital representation of objects and features based on the data fed by the sensors and aligns the representation to the digital map. In the ***acting*** phase, the computer moves the vehicle by activating its driving systems.

20. **CAVs: regulatory aspects**

Towards CAV regulation. Since the first of the UK Locomotive ('Red Flag'[51]) Acts in 1861, humans have been at the centre of vehicle road driving regulation, whether for speed limits, driving standards, driving licences, vehicle registration or roadworthiness. The removal of human control of motor vehicles that

[50] Image adapted from <https://tinyurl.com/4ueupvfr>.
[51] So called because of the early safety requirements: the Locomotives Act 1865 required road vehicles to have a three-person safety team, "one of such Persons… shall precede such Locomotive on Foot… and shall carry a Red Flag constantly displayed" (s. 3).

CAVs predicate will therefore transform over 150 years of national and international vehicle, road and traffic legislation and regulation.

The Law Commission of England and Wales and the Scottish Law Commission (the "**Law Commissions**"), in a summary report of their recent work in this area describe the change as requiring a "conceptual leap". The new reality will require drivers of traditional vehicles to overcome some fairly fundamental driving instincts and reflexes: when an automated vehicle is "self-driving", the Law Commissions conclude, "the human in the driving seat (if any) may relax and divert their attention, knowing that they are not responsible for anything that happens when the automated driving system (ADS) is engaged."[52]

UK CAV regulation: recent progress. Significant progress was made in 2022 towards the future regulatory framework for UK CAVs. Three documents were of particular importance:

- the Law Commissions' *Summary Report*, which concludes their three-year Automated Vehicles project (January 2022);[53]
- the Centre for Data Ethics and Innovation ("**CDEI**")'s *Responsible Innovation in Self-Driving Vehicles* policy paper (August 2022). This sets out a framework for a "responsible and trustworthy regulatory and assurance framework" to run alongside the Law Commissions' CAV proposals;[54] and
- the UK Government's response to the Law Commissions and the CDEI in *Connected & Automated Mobility 2025* (August 2022).[55]

The foundational components of this emerging legal framework involve: the drawing of a dividing line between merely assistive driving technologies and **automated driving systems** ("**ADS**"); a corresponding shift from the driver of a vehicle, traditionally the locus of driving control and legal responsibility, to the **user in charge** ("**UIC**") when a given ADS is engaged; a new **authorisation process** to determine whether a given driving technology should be recognised as an ADS in legal terms; and the **Authorised Self-Driving Entity** ("**ASDE**"), the manufacturer or developer that puts a vehicle equipped with an ADS forward for authorisation and takes responsibility for its actions.[56]

The next step is for the UK Government to develop legislative proposals based on these developments, which it has stated it intends to do in a forthcoming Transport Bill to be laid before Parliament in the 2022-23 parliamentary session.[57] The way the UK proposals interact with developments in the EU, and the potential for divergence will be an important factor here.[58]

CAVs: other regulatory aspects. While CAV-specific legislation looks set to redefine the 'rules of the road' in the coming years, the centrality of data and emerging technologies to developments in the CAV realm will bring CAVs squarely within the crosshairs of multiple other regulatory regimes.

---

[52] The Law Commission and the Scottish Law Commission, *Automated Vehicles: Summary of joint report*, 26 January 2022, p.2 <https://tinyurl.com/uev846mw>.
[53] The Law Commission and the Scottish Law Commission, *Automated Vehicles: Summary of joint report*, 26 January 2022 <https://tinyurl.com/uev846mw>.
[54] CDEI, *Responsible Innovation in Self-Driving Vehicles*, 19 August 2022 <https://tinyurl.com/46yu6k7v>.
[55] HM Government, *Connected & Automated Mobility 2025: Realising the benefits of self-driving vehicles in the UK*, August 2022 <https://tinyurl.com/5eap8tbm>.
[56] See further the Law Commissions *Summary Report*, Ch. 1.
[57] HM Government, *Connected & Automated Mobility 2025*, p.45.
[58] For an early example, see the following document re the impact of EU CAV rules on the position in Northern Ireland: <https://tinyurl.com/2w8s7cjs>.

Perhaps the most obvious here is data protection legislation. CAVs include a broad range of onboard devices that originate data. By some estimates CAVs can produce up to 25GBs of data per hour, much of which is personal data.[59] In January 2022, the European Data Protection Board ("**EDPB**") published guidance on the data processing aspects of CAVs in which it articulated the following privacy risks: (i) a lack of control and information asymmetry, particularly if over the life of the CAV there are multiple owners; (ii) concerns over the quality of the user's consent; (iii) concerns over further processing; (iv) concerns over excessive data collection; and (v) security concerns.[60] An explicitly governed approach to use of personal data and other data in the CAV context, consisting of statement of principles, strategy, policy and processes including tools like data protection impact assessments and privacy by design, is therefore likely to become indispensable.

Other regulatory areas of significance for CAVs are likely to be: cybersecurity; the emerging regulatory framework for AI, which will govern CAVs to the extent their systems are AI systems (see Section E); and other EU regulatory initiatives like the proposed Data Act, which among other things will provide for interoperability and data access standards for connected devices including CAVs.

D. LEGAL ASPECTS OF AI

21. **Introduction.** This section overviews relevant legal aspects of AI, aiming to develop an analytical framework that can serve as a checklist of legal areas to be considered for particular AI projects. First, some common misconceptions about AI are clarified (para D.22). AI is then briefly considered in relation to the law of intellectual property rights for software (D.23) and data (D.24), data protection (D.25), agency (D.26), contract (D.27) and tort (D.28). The emerging regulatory 'layer' for AI is discussed in Section E below.

22. **Some common misconceptions.** Three misconceptions based on the fallacy that the embodiment of AI has the qualities of a legal person[61] have clouded an analytical approach to the legal aspects of AI, where it is easy to lose sight of normal legal analysis in the glare of the unfamiliar.

    First, we all tend to anthropomorphise AI (the 'I Robot fallacy') and think of AI and robots as analogous to humans and the brain rather than as software and data.

    Second, we tend to analogise AI systems, particularly when in motion and especially in popular culture, to agents (the 'agency fallacy'). From there it is only a short jump to conferring rights on and imputing duties to these systems as agents. An agent, under present law anyway, must be a legal person so an AI system as such cannot be an agent as it is not a legal person.

    A third misconception, as AI systems increasingly interact, is to speak of these platforms as possessing separate legal personality and able to act independently of their operators (the 'entity fallacy'). Generally, under present law, the platform operator could be incorporated as a separate legal entity as a company or a partnership, where its members would be other legal entities (individuals, companies, LLPs or trusts).

[59] European Data Protection Supervisor, *TechDispatch #3: Connected Cars* (20 December 2019) <https://tinyurl.com/yc2ayse5>.
[60] EDPB, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (28 January 2020) <https://tinyurl.com/3vetnduu>.
[61] The Interpretation Act 1978 defines "person" to "include a body of persons corporate or unincorporated". Persons generally (but not always) have separate legal personality and include individuals (as natural legal persons) and bodies corporate. By s.1173 Companies Act 2006, "body corporate" and "corporation" "include a body incorporated outside the UK but do not include (a) a corporation sole, or (b) a partnership that, whether or not a legal person, is not regarded as a body corporate under the law by which it is governed".

Such an entity would behave in legal terms like any other incorporated body. If it were not itself a legal entity, it would be a partnership (as two or more persons carrying on a business in common with a view to profit) or an unincorporated association (club).

This is not to say that AI will not lead to the evolution of new types of legal entity – though the outcome of early debates on this topic suggests legal personality for AI systems is not an imminent next step.[62] The comparison would be with the development of joint stock companies in the UK's railway age, when companies were first incorporated by simple registration and then with limited liability under the Joint Stock Companies Acts 1844, 1855 and 1856.

23. **AI and intellectual property: software – works/inventions generated/implemented by computer**

Copyright. In the copyright area, UK law has always developed with new bits added on Lego-like as technology evolves.[63] A key question here concerns ownership of copyright works generated by AI systems without immediate human intervention. Here s.9(3) of the UK Copyright Designs and Patents Act 1988 ("**CDPA**") provides that:

> *In the case of a literary, dramatic, musical or artistic work which is computer generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken.*

These operative terms are fraught with difficulty. In the absence of significant case law on the point to date to clarify for example what is meant by "undertaking necessary arrangements" for the creation of the work where "there is no human author", the growing ubiquity of AI systems is likely to lead to clarification of these terms through the courts. Accordingly, parties to agreements for AI system development and use that could result in new copyright works should consider including any necessary express terms as to their ownership, assignment and licensing.

Spurred by the UK Government's recent emphasis on AI-related policymaking, the UK Intellectual Property Office ("**UK IPO**") consulted on potential changes to s.9(3) CDPA and the regime for copyright protection of computer-generated works in 2021. The options for change included scrapping protection for computer-generated works outright and reducing the scope or duration of protection under s.9(3). In its consultation response, published in June 2022, the UK Government decided to make no changes, concluding that because "the use of AI to generate creative content is still in its early stages", the impact of any legislative reform would be too uncertain.[64] Given the particularly rapid developments in AI image and video generation this year (B.11 above), it is foreseeable that this position may be revisited in the coming years.

---

[62] See the debates at the European Parliament over the last five years, for example. On 16 February 2017 the European Parliament adopted a resolution making recommendations to the Commission on civil law rules on robotics <https://tinyurl.com/4pzyj87z>. At para 59(f) the Parliament invited the Commission to "consider creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise act with third parties independently". In its package of 25 April 2018 setting out the EU's approach on AI to boost investment and set ethical guidelines, the Commission has not taken forward the Parliament's recommendation on legal personality for AI <https://tinyurl.com/bdzbcu8j>.

[63] Software was first given literary copyright protection in 1985 in the UK by the Copyright (Computer Software) Amendment Act 1985. Copyright aspects of the internet were introduced into English law by the Copyright and Related Rights Regulations 2003 (SI 2003/2498), implementing EU Directive 2001/29/EC on Copyright and Related Rights in the Information Society.

[64] UK IPO, 'Consultation outcome – Artificial Intelligence and Intellectual Property: copyright and patents: Government response to consultation', 28 June 2022 <https://tinyurl.com/4jaenh3s>.

Patents and inventions. Equally, AI use may result in new inventions and the question arises whether such computer-implemented inventions are capable of patent protection. S.1(2)(c) Patents Act 1977 ("**PA**") excludes a "program for a computer" from patent protection to the extent that the patent application "relates to that thing as such". This has led to a line of cases in the UK since 2006 which has sought to establish and clarify a test for determining the contribution that the invention makes to the technical field of knowledge (potentially patentable) beyond the computer program "as such" (not patentable).[65]

If the invention is potentially patentable on this basis, s.7(3) PA provides that:

> *[i]n this Act "inventor in relation to an invention means the actual deviser of the invention" and "joint inventor" shall be construed accordingly*

and s.7(2)(a) PA provides that a patent for invention may be granted "primarily to the inventor or joint inventors". US law is more specific in defining (at 35 USC §100(f) and (g)) "inventor" as "the individual or, if a joint invention, the individuals collectively who invented the subject matter of the invention". The context of s.7(3) means that the "actual deviser of the invention" should be a "person" and there is no regime similar to that for copyright for computer-generated works. Again, the key take away from the patent law perspective is that it is worth considering expressly covering in B2B AI contracts the ownership, assignment and licensing aspects of AI-generated inventions and patent rights as well as copyright works.

The UK IPO's 2021 AI consultation also touched on potential changes to the UK regime for patents, in particular whether the PA definition of "inventor" should be expended to include an AI system or new patent-like rights should be devised to protect inventions devised by AI systems. As with copyright for computer-generated works, the consultation outcome recommended no changes. There were two key reasons for this. First, developments in AI are at too early a stage for a clear consensus on changes to have emerged. Second, changes should be harmonised at an international level, rather than unilateral UK changes.[66]

Other recent developments have also given clarity that an AI system cannot be listed as an inventor of a patent. These are not covered here as we have written on them separately.[67]

24. **AI and intellectual property: rights in relation to data**

What is data? The initial question in respect to the datasets that AI works on is to ask: what is the nature information and data? For our purposes, information is that which informs and is expressed or communicated as the content of a message, or arises through common observation; and data is digital information. In the vocabulary of technical standards:

> ***information****… is knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning; [and]*
>
> ***data*** *is a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing [which] can be processed by humans or by automatic means.*[68]

[65] Starting with Aerotel Ltd v Teloc Holdings Ltd and Macrossan's Patent Application [2006] EWCA Civ 1371.
[66] UK IPO, Consultation outcome <https://tinyurl.com/4jaenh3s>.
[67] For instance in relation to (i) relevant updates to the UK IPO's Formalities Manual and (ii) Thaler and DABUS, both at the UK IPO and the European Patent Office. See paras E.51 to E.53 of our Algo IP: Rights in Code – 2020 Update White Paper (April 2020) at <https://tinyurl.com/52vz5zmc>.
[68] ISO/IEC Standard 2382:2015, Information technology – Vocabulary, terms 2121271 and 2121272 <https://tinyurl.com/2ptd5f53>. Information and data are used interchangeably here.

Unlike land or goods, for example, information and data as expression and communication are limitless and it would be reasonable to suppose that subjecting information to legal rules about ownership would be incompatible with its nature as without boundary or limit. Yet digital information is only available because of investment in IT, just as music, books and films (which receive legal protections through copyright and other rights) require investment in creative effort.

What is data in legal terms? Data's equivocal position is reflected in the start point for the legal analysis, which is that data is funny stuff in legal terms. This is best explained by saying there are no rights ***in*** data but that rights arise ***in relation to*** data. The UK criminal law case of *Oxford* v *Moss*[69] is generally taken as authority for the proposition that there is no property ***in*** data as it cannot be stolen; and that the 2014 *Your Response*[70] case confirmed that a lien (a right to possession of a good as a tangible thing) does not subsist over a database because the database is intangible and so there is no good to possess. However, the rights and duties that arise ***in relation to*** data are both valuable and potentially onerous and are likely to develop as AI techniques predicated on processing very large datasets become more established.

IPR, contract and regulatory rights and duties in relation to data. These rights and duties in relation to data arise through intellectual property rights ("**IPR**"), contract and regulation. They are important as (positively, in the case of IPR and contract) they can increasingly be monetised and (negatively) breach can give rise to extensive damages and other remedies (for IPR infringement and breach of contract) and fines and other sanctions (breach of regulatory duty).[71] Current developments in each of these areas mean that 'data law' has emerged as a new area in its own right around these three constituents of IPR, contract and regulation. This can be modelled in the AI context as the middle four layers of an 8-layer stack, sandwiched between AI platform infrastructure and information architecture below and data ethics, governance and security above (Figure 7 below).

[69] [1979] Crim LR 119, where it was held that confidential information in an exam question was not "intangible property" within the meaning of Section 4(1) of the Theft Act 1968 and so could not be stolen.

[70] *Your Response Ltd* v *Datateam Business Media Ltd*, judgment of the Court of Appeal on 14 March 2014 [2014 EWCA 281]; [2014 WLR(D) 131]. A lien is a possessory remedy available only for things (or "choses") in possession – i.e. personal tangible property. A database is a thing (or "chose") in action – i.e. ultimately capable of enjoyment only through court action.

[71] For a more in-depth review of the technical aspects of data see our *Legal Aspects of Managing Data White Paper* (October 2019) <https://tinyurl.com/5yf2rb79> and Richard Kemp et al, *Legal Aspects of Managing Big Data* (30 CLSR [5]) <https://tinyurl.com/45mfydkz>, pp. 482-491.

Figure 7: Towards a common legal framework for data

Level 8: data governance & management	• Standards: ISO 38505 (data governance), 29134 (cloud data flows), etc; data sharing strategy, policy and best practice
Level 7: information security	• generally applicable: NIS Regulation, data residency, etc. • best practice: technical standards: ISO 27001, SSAE 16/18, etc.
Level 6: regulation of personal data	• GDPR, PECR compliance, etc.
Level 5: data regulation (other than personal data)	• non-sector specific: competition law, duty of care • sector specific: financial services, professional services, etc.
Level 4: contracting for data	• 'contract is king' – protection strong (strict liability) but limited ('*in personam*' – only contracting parties)
Level 3: IP rights in relation to data	• copyright, database right, confidence/know-how, patents • protection extensive ('*in rem*') but uncertain (as to data)
Level 2: information architecture	• data structure, design, schemas, format • data model as representation of data flows
Level 1: AI platform infrastructure	• software: OS, database middleware, AI software algorithms, BI & analytics applications

Rights in relation to data: practical challenges. The April 2018 House of Lords report *AI in the UK: ready willing and able?* Illustrates the challenges that arise for data in the AI context. Here the question (no. 56) that the Committee considered was:

> *Who should own data and why? Is personal ownership of all data generated by an individual feasible and if so how?*

and they came to the view that:

> *data control was a more appropriate concept [than data ownership… and] we have accordingly decided to refer to data control, rather than ownership,*

noting the assertions given in evidence that:

> *data has a few qualities that make it incompatible with notions of ownership. I can hold it, you can hold it, and my holding of it does not impact the value you can derive from it…*[72]

That different people can hold data without impacting its value is little different from the case of software, which copyright protects as a computer program:[73] that data is inherently boundaryless is not in principle incompatible with the legal rights of ownership. The *Your Response* case is clearly correct on the point that a database, as an intangible, cannot give rise to a lien but the case does not say there is no property in a database, just that there is no tangible property.

So these assertions do not necessarily support the proposition that data cannot be subject to rights of ownership. The technical ingredients of copyright, database right, confidence/know-how and patents are specific to each right, complex and vary from country to country. There is currently also a lively policy

[72] House of Lords Select Committee on Artificial Intelligence, AI in the UK: ready, willing and able?, HL Paper 100 (April 2018), <https://tinyurl.com/2p8xw8b7>, p. 28.
[73] CDPA, s. 3(1)(b).

debate around open source, open data and how far IPR protection should extend in these times of exponential growth in digital data volumes. But if, within their limits, the ingredients of a particular right are present on ordinary principles, that right may apply in relation to data, just as it may apply to software or text and just as data may be subject to contract and regulatory rights and duties. Finally, to speak in terms of 'data control' or 'data ownership' in a binary 'either/or' sense is to set up a false dichotomy: legal ownership rules in relation to data and rights and power in exercise of control over that data exist alongside each other but are independent.

The discussion in the House of Lords report illustrates the challenges and uncertainties around data as a developing area of law. The take away from the data perspective is that parties to B2B AI contracts should consider and expressly provide for the ownership, assignment and licensing aspects of all relevant datasets (training, testing and other input datasets; output datasets; derivative datasets) and processing.

Trade secrets and database right. We have written elsewhere about the growing importance of trade secrets and database right for AI, algorithms and their related datasets.[74]

25. **AI and data protection**

AI and the UK GDPR[75] generally. Since its coming into effect in 2018, the UK GDPR has affected the development and deployment of AI systems more than any other single piece of regulation. The start point for the privacy analysis is that the GDPR applies to the AI-enabled processing of personal data just as it does to other forms of processing. Former Information Commissioner Elizabeth Denham acknowledged this in her foreword to the Information Commissioner's Office's ("**ICO**") July 2020 *Guidance on AI and Data Protection*:

> *the underlying data protection questions for even the most complex AI project are much the same as with any new project. Is data being used fairly, lawfully and transparently? Do people understand how their data is being used? How is data being kept secure?*[76]

But the ICO has also acknowledged the specific risks AI poses. Certain aspects of AI, it writes, "have implications for data protection and privacy" which "distinguish it from more traditional processing". In particular, AI has the following "distinctive aspects": (i) the use of algorithms; (ii) the opacity of the processing; (iii) the tendency to collect 'all the data'; (iv) the repurposing of data; and (v) the use of new types of data.[77]

The ICO's AI focus. As a result, the ICO has identified AI as a priority area and is focusing in particular on the following aspects of AI: (i) fairness in AI; (ii) dark patterns; (iii) AI-as-a-service; (iv) AI and recommender systems; (v) biometric data and biometric technologies; and (vi) privacy and confidentiality in explainable AI. The ICO has also published several pieces of AI-specific guidance and tools in recent years, including the:

[74] See paras E.47 and E.48 of our Algo IP: Rights in Code – 2020 Update White Paper (April 2020) <https://tinyurl.com/52vz5zmc>.
[75] I.e. the retained EU law version of GDPR as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419). In citing UK GDPR in this section, we have referred to DCMS's GDPR Keeling Schedule (available at <https://tinyurl.com/29aw7z6t>).
[76] ICO, *Guidance on AI and Data Protection* <https://tinyurl.com/3ssv6tzw>.
[77] ICO, *Big data, artificial intelligence, machine learning and data protection* (September 2017) <https://tinyurl.com/ypujycsa>, p. 9.

- *AI and data protection risk toolkit v.1.0* (May 2022);[78]
- *Guidance on AI and Data Protection* (July 2020);[79] and
- *Explaining Decisions made with AI* guidance, a collaboration with the Alan Turing Institute (May 2020).[80]

These documents form a substantial part of the ICO's recent response to AI and are recommended reading for those looking for an overview of the topic. The remainder of this section is confined to the following AI-specific issues for data protection: (i) the borderline between data processors and data controllers in the AI context; (ii) anonymisation as a compliance tool for AI projects; (iii) and profiling and automated decision-making.

AI projects (i) – AI provider as data processor or data controller? By UK GDPR Art. 4(7) a person who determines the "purposes and means" of processing personal data is a data controller and under the UK GDPR the data controller bears primary responsibility for the personal data concerned. By Art. 4(8), a data processor just processes personal data on behalf of the data controller. Although the data processor does not have direct duties to data subjects for that data, it is required under Arts. 28 to 32 to accept prescriptive terms in its contract with the controller and to take certain other measures. Essentially, an AI provider as controller has direct duties to the data subjects but as a processor just has direct duties to the controller. Correctly characterising the AI provider as processor or controller is therefore critical to UK GDPR-compliant structuring of the relationship and to allocating risk and responsibility.

But, in practice, the borderline between controller and processor can be fuzzy. The ICO notes that the "definition of a processor can be difficult to apply in the complexity of modern business relationships".[81] This is especially so for AI, where networks of processors can interact with each other in complex and multifaceted ways. A key point is that the analysis depends on the processing activity in question, and can be different across different processing activities.

The correct approach to categorising controllers and processors when AI is involved is a developing area. The ICO plans to consult and release further guidance on this question as part of its review of its cloud computing guidance.[82]

AI projects (ii) – anonymisation as a compliance tool. Anonymisation is a powerful compliance tool in the AI context because anonymous information is outside the scope of the UK GDPR. As UK GDPR Recital 26 states:

> *The principles of data protection should… not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.*

[78] ICO, *AI and data protection risk toolkit v.1.0* (May 2022) <https://tinyurl.com/42vnpuvn>. The toolkit offers specific guidance for organisations' use of AI systems. It sits alongside, but does not replace, the data protection impact assessment which is generally required when AI is used.
[79] ICO, *Guidance on AI and Data Protection* (July 2020) <https://tinyurl.com/3ssv6tzw>.
[80] ICO, *Explaining decisions made with AI* (May 2020) <https://tinyurl.com/3tbp6a68>.
[81] ICO, 'How do you determine whether you are a controller or processor?' <https://tinyurl.com/2k9p27yn>. See also: European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (adopted on 02 September 2020) <https://tinyurl.com/2p99bhvm>.
[82] ICO, 'What are the accountability and governance implications of AI?' <https://tinyurl.com/j6vw8xa5>.

Three further points are worth noting here. First, that the act of anonymising personal data is itself a processing activity that falls within scope of the UK GDPR – so this activity requires the data controller to have a lawful basis for the processing.[83] Second, that UK GDPR sets a high bar for what constitutes 'genuinely' anonymous information and the boundary line between personal data and anonymous information can be difficult to identify with certainty. Third, that the growing body of regulatory guidance published both by the ICO and European privacy regulators (in respect of EU GDPR) suggests that regulators have different views on what anonymous information is.

Recent expressions of the GDPR anonymisation 'standard' from the ICO and other supervisory authority illustrate these points. For the UK GDPR, the ICO has recently appeared to take a pragmatic view on anonymisation – not setting the bar unreachably high. In its anonymisation guidance (in draft form at the time of writing), the ICO states that "effective anonymisation is about finding the right balance between managing the risk while keeping the utility of the data… you can adopt a certain amount of pragmatism."[84] For Germany's Federal Commissioner for Data Protection and Freedom of Information, for data to be anonymous re-identification needs to be "practically impossible".[85]

For the lawyer advising on anonymisation of personal data in the context of AI systems, articulating the requirements of effective anonymisation to product teams will be important.

AI projects (3) – profiling and automated decision-making. AI's ability to uncover hidden links in data about individuals and to predict individuals' preferences can bring it within the UK GDPR's regime for profiling and automated decision-making, defined by Art. 4(4) as:

> *any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.*

Art. 22(1) extends data subjects' rights to "decisions based solely on automate processing":

> *the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

The right is qualified not absolute and by Art. 22(2) does not apply if the decision:

> *(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
>
> *(b) is required or authorised by domestic law which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
>
> *(c) is based on the data subject's explicit consent.*

The requirement for decisions to be based "solely" on automated processing is leading AI users to consider interposing human evaluation between the machine and the data subject. The tension between the UK GDPR's requirements and the costs of human intervention in this way may lead to claims about the quality

[83] See further: ICO, *Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance – Vol. 1 – Introduction to Anonymisation*, p.12 <https://tinyurl.com/5xwf4jy3>. As at the date of publication, this guidance was in draft form.
[84] ICO, Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance – *Vol. 2 – How do we ensure anonymisation is effective?*, p.12 <https://tinyurl.com/e8czyjsr>.
[85] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche* (29 June 2020), p. 4.

and genuineness of the human decision making. In this regard, the ICO states that "the human involvement has to be active and not just a token gesture".[86]

26. **AI and agency law**

Agency is a relationship between two legal persons. In the words of the leading work on UK agency law, it is:

> *the fiduciary relationship which exists between two persons, one of whom expressly or impliedly manifests assent that the other should act on his behalf so as to affect his legal relations with third parties, and the other of whom similarly manifests assent so to act or so acts pursuant to the manifestation.*[87]

As mentioned at D.22 above, a common misconception is to regard AI systems as 'agents' who act for their 'principal'. An AI system is not of itself a legal person. It – or rather the personal property (goods) and intangible rights (intellectual property rights in software and data) it consists of – belongs to the system's owners and is possessed by and provided as a licence or a service to the user.

27. **AI and contract law**

Commercial contracts for the development and use of B2B AI systems between developer/licensor/provider and licensee/customer will, in the short term, be broadly similar to other software contracts, whether provided on-premise as a licence or in-cloud as a service. Similar issues to those in software and data licences and agreements will need to be addressed in AI agreements and are not considered further here.[88] Equally, mass market B2C AI services (like digital personal assistants) will continue to be made available to subscribers through click accept licensing terms. However, as the regulatory landscape for AI crystallises in the coming years, we expect to see – as an emerging trend – contracts dealing with AI adopt concepts and approaches taken in AI legislation.

The legal analysis becomes more complex in the case of smart contracts. Blockchain/DLT-enabled smart contracts will have the ability to make, virtually real time, interlocking chains of contracts linked by dependencies. For each link in the chain the requirements of contract formation in the jurisdiction(s) that govern the smart contract ecosystem will need to be met, both as code (the software code that implements the system) and contract (in the agreement governing use). In the UK these include: (i) that each party has legal capacity; (ii) intention to create legal relations; (iii) offer; (iv) acceptance; (v) communication of acceptance; (vi) consideration; (vii) obligations recognised by law; and (viii) certainty of terms.

Where the chain of contracts becomes extended, the possibility arises that an earlier contractual link will be broken, for example, because the contract formation requirements were not met or the contract was discharged through breach. The impact of a broken upstream contractual link on a downstream contract in an AI-enabled or smart contract system is likely to raise novel contract law questions. An agreement may lack contractual force for uncertainty[89] or any downstream contractual link in the chain may be dependent – as a condition precedent – on the performance of all anterior upstream agreements. An

[86] ICO, '*What does the UK GDPR say about automated decision-making and profiling?*' <https://tinyurl.com/2svp5yu6>.
[87] Peter Watts and F.M.B. Reynolds, *Bowstead and Reynolds on Agency*, twenty second edition (London: Sweet & Maxwell, 2021), p.1.
[88] See further our white paper *Demystifying Tech for non-Tech Lawyers* (March 2021) at < https://tinyurl.com/mryeudhr>. See also our *Tech Law Trends 2022* (January 2022) at <https://tinyurl.com/2kw6kjfy>.
[89] Hugh G. Beale, *Chitty on Contracts*, thirty fourth edition (London: Sweet & Maxwell, 2021), para 4-185.

almost limitless range of possibilities will need to be addressed in software terms in the smart contract code base and covered in the express contractual terms of the "house rules" that govern the use of the system. It is therefore foreseeable that contract law will evolve in this area as novel smart contract system disputes arise and are settled through the courts.

Smart contracts will pose novel questions for contract law, but established principles are also likely to continue to apply. For UK law at least there is a growing consensus that "current legal principles can apply to smart legal contracts in much the same way as they do to traditional contracts."[90]

28. **AI and tort law: product liability, negligence, nuisance and escape**

Importance of tort law for AI. Outside regulatory and statute law, it is perhaps the common law of tort that is most likely to see the most important AI-influenced developments. Product liability will evidently also be relevant for autonomous vehicles, robots and other 'mobile' AI-related or autonomous systems, and the tort of breach of statutory duty may also apply depending on the regulatory backdrop. The AEVA, in extending the compulsory insurance regime for ordinary vehicles to listed CAVs, specifically refers to contributory negligence, and this shows the interplay between tort law and statute. Recent EU proposals in relation to the liability regime for AI are considered in Section E below.

Negligence. Negligence under English law centres on the existence of a duty at common law "to be careful". The list of situations giving rise to a duty of care is famously not fixed: in the words of the UK House of Lords in the UK's leading case, "the categories of negligence are never closed"[91], and it is hard to imagine that the common law duty of care will not arise in relation to many, or most, kinds of AI.

Moreover in a world where an AI system's ability to diagnose a disease or drive a car surpasses human ability, how is the standard of care in negligence to be assessed? If it becomes commonplace for doctors to use AI tools in diagnostic procedures because AI tools are so much more accurate, would the doctor that refuses to do so and then fails to spot an issue be negligent because the reasonable thing to have done would have been to use the AI tool?[92]

Nuisance and escape. Nuisance and escape (*Rylands* v *Fletcher*) liability are based on interference with the use or enjoyment of land, and are more likely to be relevant for robots, autonomous vehicles and other kinds of 'mobile AI' than for 'static AI' systems. If a robot runs amok, the situation may be analogised to straying animals where under English law liability has been codified by statue under the Animals Act 1971, s.4 of which for example imposes strict liability for straying animals. This points back to statutory regulation of AI but, for the moment, one can easily imagine the common law being extended to treat AIs causing unreasonable annoyance to a neighbour as nuisance in the same way as for animals.

The rule in *Rylands* v *Fletcher* is that:

> *a person who for his own purposes brings on his lands and collects or keeps there anything likely to do mischief if it escapes must keep it in at his peril, and if he does not do so, is prima facie answerable for all damage which is the natural consequence of its escape.*[93]

[90] Law Commission, *Smart legal contracts: Advice to Government* (November 2021) <https://tinyurl.com/2k5c2c7r>, p.5.
[91] Lord Macmillan in Donoghue v Stevenson [1932] A.C. 562 at p. 619.
[92] See discussion in Matthew Lavy and Iain Munro, 'Liability for Economic Harm' in *The Law of Artificial Intelligence*, ed. by Matt Hervey and Matthew Lavy (London: Sweet & Maxwell, 2021), pp. 153-186, p.175.
[93] (1866) L.R. 1 Ex. 265 at p. 279.

The principle extends to "dangerous things" as "things" "likely to do mischief" on escape and has been applied to motor vehicles and electricity but not to an aeroplane or a cricket ball driven out of the ground.[94] Extending *Rylands* v *Fletcher* escape liability in tort to AI would therefore appear to be a relatively simple extension consistent with past decisions.

E. AI REGULATION

29. **Introduction.** This section looks at the emerging regulatory and policy landscape for AI across three geographies:

- First, the EU where the AI regulatory framework is rapidly taking shape thanks to several proposed sets of rules – the AI Act (E.30) and AI Liability Directive (E.31) in particular, but also the broader sweep of incoming digital regulation as part of the EU's Digital Strategy programme (E.32).
- Second, the US which, in its apparent preference for incremental sector-specific regulation, is a counterpoint to the EU's approach (E.33).
- Third, the UK, where the AI regulation debate has for the time being come out firmly in favour of a 'light touch' 'pro-innovation' approach (E.34).

This section is about regulations that have AI as their primary focus. For 'background' legislation which nevertheless has implications for AI (e.g. IP and data protection law) see Section D above.

30. **EU Developments (1): the AI Act**

General approach. The European Commission's proposal for an 'AI Act' – taking the form of a Regulation setting out detailed AI-specific rules[95] – has been the subject of intense negotiation since it was put forward in April 2021. Notably, more amendments have been proposed to the AI Act (4,852) than were put forward during the entire legislative process for the GDPR (4,027).[96] This section cites the latest draft of the AI Act at the time of writing (the fourth proposed compromise text from 19 October 2022).[97]

The AI Act proposes a 'horizontal' approach to AI regulation. This means the proposals would apply to "AI systems" and various actors involved in the process of developing, importing and using AI systems, regardless of industry sector. This is as opposed to a 'vertical' approach that would apply AI rules on a 'sector specific' basis – different rules for the healthcare and financial services sectors, for instance.

The AI Act centres around the concept of the "AI system", which is currently defined (at Art. 3(1)) as:

> *a system that is designed to operate with elements of autonomy and that, based on machine and/or human provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.*

The current proposals take a "risk-based approach" to AI systems. First, the AI Act sets out a category of **prohibited AI practices**, which are banned outright. Then follows a category of **high-risk AI systems** which

[94] Motor car – *Musgrove* v *Pandelis* [1919] 2 K.B.43; electricity – *National Telephone Co.* v *Baker* [1893] 2 Ch. 186; aeroplane – *Fosbrooke-Hobbs* v *Airwork Ltd* [1937] 1 All E.R. 180; cricket ball – *Bolton* v *Stone* [1951] A.C. 850.
[95] See the Commission's original proposals here: <https://tinyurl.com/23yr33kw>.
[96] Source: https://parltrack.org/. 4,852 figure for the AI Act <https://tinyurl.com/4aj3ruzx>. 4,027 figure for the GDPR <https://tinyurl.com/5ajy8rx4>.
[97] Available here: <https://tinyurl.com/3cfyhsj8>.

are subject to specific rules. There are also **transparency obligations** for certain AI systems, among other things. In keeping with the approach taken in the GDPR, the AI Act also features potentially large **monetary penalties** for breach.

Prohibited AI practices. The proposed AI Act sets out (at Art. 5) a category of AI practices which is banned outright, because they are deemed to be incompatible with the fundamental values (respect for human dignity, freedom, equality, democracy and the rule of law) and rights (including the right to non-discrimination, data protection and privacy and the rights of the child) of the EU.

The current list of prohibited AI practices is summarised at Table 1 below.

High-risk AI systems. Next, the proposals set out a category of AI systems which are deemed to be 'high risk' (Art. 6) and, as such, would be subject to a range of granular compliance-type obligations (Arts. 8 – 15). The "Provider" of a high-risk AI system (the person that "develops an AI system" and "places that system on the market") attracts further specific obligations (Arts. 16 – 25), as do "importers" (Arts. 26 – 28) and "users" (Art. 29) (the "user" of a high-risk AI system being the entity "under whose authority the system is used").

Whether an AI system is "high-risk" or not is determined (in Art. 6) by reference to a list of technologies (set out in Annex III) which the European Commission has the ability to amend from time to time as new "high-risk" applications of AI emerge (Art. 7).

Transparency obligations. By Art. 52, where an AI system is "intended to interact with natural persons" the provider must ensure it is designed so that those natural persons are "informed that they are interacting with an AI system" by the time they first interact or are exposed to the AI system.

Monetary penalties. The proposed AI Act sets out a three-tiered approach to administrative penalties for companies. The level of the penalty is expressed to take into account the "size and interests of SME providers, including start-ups and their economic viability" so presumably smaller actors would get lower fines, but how this works in practice remains to be seen.

Nature of breach	***Maximum administrative penalty***
Breach of Art. 6 (prohibited AI practices)	Higher of **EUR 30 million** or **6%** of total worldwide annual turnover for preceding financial year
Breach of core provider / importer / distributor / authorised representative obligations	Higher of **EUR 20 million** or **4%** of total worldwide annual turnover for preceding financial year
Supplying incomplete, incorrect or misleading information to authorities	Higher of **EUR 10 million** or **2%** of total worldwide annual turnover for preceding financial year

Table 1: General approach of the proposed EU AI Act[98]

Prohibited AI Practices (Art. 5)
1. AI systems that use **subliminal techniques** which distort a person's behaviour and cause harm. 2. AI systems that **exploit vulnerabilities** (e.g. age / disability) which distort behaviour and cause harm. 3. Some forms of **social scoring** AI systems that lead to detrimental or unfavourable outcomes.

[98] Table 1: General approach of the proposed EU AI Act is a summary. It does not follow the text of the proposed AI Act exactly.

4. **Real-time remote biometric identification systems** by law enforcement, with narrow exceptions.	
High-risk AI systems (Arts. 6 – 29 and Annex III)	
High-risk AI systems (Annex III)	***Requirements for high-risk AI systems (Arts. 8 – 15)***
1. Remote biometric identification systems 2. Safety components in critical infrastructure 3. Some educational and vocational training use cases 4. Some recruitment and employment use cases 5. Determining access to essential public (e.g. benefits) / private (e.g. credit) services 6. Some law enforcement use cases 7. Some migration, asylum, etc. use cases 8. Some administration of justice use cases	1. Conformity assessment 2. Risk management system 3. Quality of input / testing data 4. Detailed technical documents 5. Records / automatic logs 6. Transparency & provision of information to users 7. Human oversight 8. Accuracy, robustness and cybersecurity requirements Additional obligations for providers, distributors, importers, users and others are set out in **Arts. 16 – 29)**

31. **EU Developments (2): the AI Liability Directive and the revised Product Liability Directive.** The AI Act (E.30 above) sets out a broad suite of measures aimed at stopping the harms that could be caused by AI systems from arising in the first place. However the AI Act does not itself propose any new rights for individuals that are adversely affected by such systems in practice.[99] This, it is argued, puts individuals on the receiving end of an unfair decision caused by an AI system at an unfair disadvantage. This contrasts with the powerful rights afforded to data subjects under Chapter III of the GDPR[100] in in relation to the processing of their personal data.

This gap is to be filled by the European Commission's proposed revisions to the European regime for civil liability, which take the form of two proposed new Directives: the **AI Liability Directive**[101] and the **revised Product Liability Directive**,[102] first drafts of which were both published by the Commission on 28 September 2022.

AI Liability Directive. The AI Liability Directive would be closely related to the AI Act, borrowing core definitions ("AI system", "high-risk", "provider", etc.) and cross-referring to its provisions. The central premise of the AI Liability Directive is that "the specific characteristics of certain AI systems, such as opacity, autonomous behaviour and complexity" could make it overwhelmingly difficult for individuals who suffer loss or damage at the hands of an AI system to "prove that a specific input for which the potentially liable person [e.g. the "provider" of the AI system] is responsible had caused a specific AI system output that led to the damage at stake" (Recital 3). To redress this potential imbalance, the Directive makes two proposals:

[99] See further: Lilian Edwards for the Ada Lovelace Institute, *Regulating AI in Europe: four problems and four solutions* (31 March 2022) <https://tinyurl.com/2s4dx2nr>, pp.10-11.
[100] I.e. the rights: to be informed (GDPR, Arts. 13 – 14); of access (Art. 15); of rectification (Art. 16); to be forgotten (Art. 17); to restrict processing (Arts. 18 - 19); to data portability (Art. 20); and to object to automated decision-making (Art. 21).
[101] See further: European Commission, *proposed AI Liability Directive* [COM(2022) 496 final] <https://tinyurl.com/5xzas58p>.
[102] See further: European Commission, *proposed new Product Liability Directive* [COM(2022) 495 final] <https://tinyurl.com/48cfysb3>.

- First, at Article 3 a mechanism by which the national courts of a Member State can compel the disclosure of evidence relating to a high-risk AI system that is suspected of having caused damage to a claimant or potential claimant.
- Second, at Article 4 a rebuttable presumption of a causal link between the fault of a defendant (e.g. the "provider" of an AI system) and the output or failure to provide an output of its AI system.

Revised Product Liability Directive. At a high level, the revised Product Liability Directive extends product liability rules to cover digital products, and works alongside the AI Liability Directive. In the words of the Commission, its aim is to "modernise and reinforce the current well-established rules, based on the strict liability of manufacturers for the compensation of personal injury, damage to property or data loss caused by unsafe products."[103]

32. **EU Developments (3): other developments in the EU's Digital Strategy.** Finally, a word on the broader proposals for tech regulation put forward as part of the EU's Digital Strategy and Policy Programme. Remarkably, in addition to the three AI-specific sets of rules discussed above (the AI Act (E.30), the AI Liability Directive and the revised Product Liability Directive (E.31)), there are no fewer than six other major new sets of tech and data related rules either proposed, in transition or in force. These changes, perhaps the most vigorous regulatory response to emerging technologies in history, will also have significant implications for AI (though they are outside the scope of this white paper[104]).

33. **AI regulation in the US.** Although the US has been taking a keen interest in the passage of the AI Act through the European legislative process[105], progress on AI policy and regulation in the US looks rather different from that in Europe. There are two key differences. First, progress has been slower and the US does not appear to be taking such a proactive approach to regulation. Second, and perhaps more significant over the longer term, the US appears to be taking a 'vertical' approach (i.e. sector-specific) as opposed to the EU's 'horizontal' approach.

In October 2022, the White House Office of Science and Technology Policy ("**OSTP**") published its *Blueprint for an AI Bill of Rights* ("**AI Bill of Rights**"), a non-binding "national values statement and toolkit" setting out five high-level principles for the deployment of AI systems and associated technical guidance for implementing these principles in practice, as summarised in Table 2 below.[106] While it is non-binding, its lasting impact may be the way it influences the development of sector-specific rules for AI at the level of US Federal Agencies.[107]

Table 2: Summary of US AI Bill of Rights Principles

#	*Principle*	*Outcome*
1.	Safe and effective systems	You should be protected from unsafe or ineffective systems.
2.	Algorithmic discrimination protections	You should not face discrimination by algorithms and systems should be used and designed in an equitable way.

[103] European Commission press release, *New liability rules on products and AI to protect consumers and foster innovation* (28 September 2022) <https://tinyurl.com/2s4hxs9p>.
[104] See our Tech Law Trends for 2023 blog for more on this: <https://tinyurl.com/34w9kfnu>.
[105] See further: Euractiv.com, *The US unofficial position on upcoming EU Artificial Intelligence rules* (26 October 2022) <https://tinyurl.com/y4ujxp76>.
[106] OSTP
[107] See further: Alex Engler, Lawfare Blog, *The AI Bill of Rights Makes Uneven Progress on Algorithmic Protections* (7 October 2022) <https://tinyurl.com/ynbb8nmy>.

#	Principle	Outcome
3.	Data privacy	You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used
4.	Notice and explanation	You should know that an automated system is being used and understand how and why it contributes to outcomes that impact you.
5.	Human alternatives, consideration and fallback	You should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter.

34. **AI regulation in the UK.** The UK Government's July 2022 Policy Paper *'Establishing a pro-innovation approach to regulating AI'*[108] is the most significant recent articulation of its approach to AI regulation. The Policy Paper is expressly (it might not be going to far to say 'relentlessly') pro-innovation in its approach.

    Unlike the specific liability framework for AI systems proposed in the EU (E.31 above), the UK Government does not intend to create "an extensive new framework of rights for individuals" in relation to AI. Sector-specific regulators, which would be tasked with implementing a set of high-level but non-binding principles, will be encouraged "to consider lighter touch options" before putting mandatory rules in place, "for example, through a voluntary or guidance-based approach for uses of AI that fall within their remit."

    Accordingly, there is not too much to say on the UK AI regulatory front at present. The one caveat to this is technical standards. While the July 2022 Policy Paper lacks a grand regulatory vision, it is keen to point out the international context for AI, and in particular the importance of "work[ing] closely with partners" to "prevent a fragmented global market, ensure interoperability and promote the responsible development of AI internationally". Thus, a specific ambition of the Policy Paper is to "ensure that UK industry's interests are well represented in international standardisation – both to encourage interoperability and to embed British values." This ambition has culminated in the launch, in October 2022 of the AI Standards Hub,[109] a body which aims to help interested parties use, understand and develop technical standards for AI.

F. AI IN THE ORGANISATION: ETHICS AND GOVERNANCE

35. **Introduction.** After a flurry of AI codes of conduct and guidelines from both government and AI industry stakeholders in the period up to c.2020, we have noticed a slowdown in the number of new guidance-type publications on AI in the last couple of years. This is likely to be due to the combined effects of market saturation and the fact that key jurisdictions (the EU in particular) have since turned their attention to 'hard' rules on AI.

    Since the last version of this White Paper (February 2021), the UK government's key output has been:

    - the *AI and Data Protection Risk Toolkit*, developed by the ICO (May 2022);[110] and

[108] Department for Business, Energy and Industrial Strategy et al, *Establishing a pro-innovation approach to regulating AI* (20 July 2022) <https://tinyurl.com/bdhtezxm>.
[109] See further: AI Standards Hub website <https://tinyurl.com/35f55km8>.
[110] ICO, *AI and Data Protection Risk Toolkit* <https://tinyurl.com/42vnpuvn>.

- v.1.2 of the *Algorithmic Transparency Standard*, developed by the Cabinet Office's Central Digital and Data Office ("**CDDO**") and the CDEI (October 2022).[111]

These publications are the latest in a growing corpus of UK Government AI ethics guidance. There have also been some important multilateral developments, including:

- the OECD's *Principles on Artificial Intelligence* (May 2019);[112] and
- the G20's *AI Principles* (June 2019).[113]

36. ***AI governance – general.*** Beginning with Open-source Software ("**OSS**") governance 20 or so years ago, a structured approach to IT-related governance has become widely accepted in private sector organisations. Broadly, there are three pieces to this type of governance: (i) a statement of strategy or high-level principles; (ii) a statement of policy to implement the principles; and (iii) the nuts and bolts of processes to anchor the policy into the organisation's operations. Structured IT governance received a boost in the era of data protection as organisations operationalised GDPR compliance, and it is likely over time that organisations will move towards a comprehensive approach to governance for all their data use cases across the business.

The UK Government, as the UK's largest user of IT, has been at the forefront of developing structured governance in this area, for example in the area of the cloud as regards data classification and cloud security. We have suggested elsewhere that private sector organisations may consider the UK Government's approach to the cloud as a basis for their own cloud migration operations as much of the heavy lifting has been done and the guidance is comprehensive and accessible.[114]

We suggest organisations may consider taking a similar approach for AI and data ethics and follow the lead of large technology developers in the case of AI principles (F.37) and operationalising AI principles (F.38) and the UK Government or AI and data ethics policy and processes (F.39).

[111] CDDO and CDEI, *Algorithmic Transparency Standard v1.2*, available on GitHub: <https://tinyurl.com/bdeapypd>.
[112] Available here: <https://tinyurl.com/2zfv42d5>.
[113] Available here: <https://tinyurl.com/37hcz6aw>.
[114] See Kemp IT Law, *Legal Aspects of Cloud Computing: Cloud Security* (June 2018) <https://tinyurl.com/2p98fse8>, para C.19.

Table 3: AI Principles - Microsoft (January 2018) and Google (June 2018)

#	Microsoft – AI Principles[115]	Google – AI Principles[116]
1.	**Fairness**: AI systems should treat all people fairly	AI should **avoid creating or reinforcing unfair bias**
2.	**Reliability and Safety**: AI systems should perform reliably and safely	AI should **be built and tested for safety**
3.	**Privacy and Security**: AI systems should be secure and respect privacy	AI should **incorporate privacy design principles**
4.	**Inclusiveness**: AI systems should empower everyone and engage people	AI should **be socially beneficial**
5.	**Transparency**: AI systems should be understandable	AI should **uphold high standards of scientific excellence**
6.	**Accountability**: People should be accountable for AI systems	AI should **be accountable to people**
7.		AI should **be made available for uses that accord with these principles**

37. **AI principles.** Both Microsoft and Google published in 2018 a set of principles to guide AI development, and these are set out at Table 3 above. Although couched in different terms, they each seek to promote fairness, safety and reliability, privacy and security, inclusiveness, transparency and accountability. They could be a useful start point for the organisation's own statement of AI principles.

38. **Operationalising AI principles.** Since the publication of their AI principles in 2018, Microsoft and Google (among others) have each published a range of documents and tools aiming to demonstrate how they 'operationalise' their AI principles – i.e. bridge the gap between principles and product. For instance in June 2022, Microsoft published v2 of its 'Responsible AI Standard' which provides "concrete and actionable guidance as to what [Microsoft's] principles mean and how [Microsoft's product development teams] could uphold them".[117] Microsoft also maintains a series of 'Transparency Notes' aiming to provide customers "with information about the intended uses, capabilities and limitations of [its] AI platform services".[118] These documents could provide a useful starting point for organisations looking to put AI principles into practice.

39. **AI governance – the UK government's data ethics framework.** The UK Government, as the steward of the country's largest datasets, is also at the forefront of ethics, best practice and governance for AI.

    The Government Digital Service's Data Ethics Framework, (now in its third edition) sets out key principles for appropriate use of data in the public sector. The Framework is designed to be able to be overlaid onto data-focussed public sector projects. There are two key parts to its structure:

[115] Microsoft, *Microsoft Responsible AI Principles* <https://tinyurl.com/53683mc6>. Microsoft's AI Principles appeared in an earlier form in Brad Smith and Harry Shum, *The Future Computed: Artificial Intelligence and its Role in Society* (January 2018) <https://tinyurl.com/3x3z96rw> , pp.51–83.

[116] Google, *Artificial Intelligence at Google: Our Principles* <https://tinyurl.com/ywc4p22h>. Google also espouses four 'negative' principles of AI design and deployment that it will not pursue. These are technologies that: (i) cause or are likely to cause overall harm; (ii) for weapons, etc.; (iii) for surveillance that violates internationally accepted norms; and (iv) breach the principles of international law and human rights.

[117] Microsoft, *Responsible AI Standard*, v2 (June 2022) <https://tinyurl.com/sfcmjdzd>, p.3.

[118] Microsoft, 'Transparency Notes' <https://tinyurl.com/4xaeunsk>.

- First, three **overarching principles** that underpin all aspects of the project: (i) transparency, (ii) accountability, and (iii) fairness.
- Second, five **specific actions** that apply at different stages of the project.

We suggest this Framework, with some adaptation for commercial considerations, could be used by private sector organisations as a start point for the policy and process elements of their own data ethics and governance. The Framework also includes a helpful editable template which it states should assist public sector teams to record the ethical decisions they have taken about their projects. Table 4 below sets out the principles, specific actions and areas of additional guidance.

40. **AI and technical standards.** Finally a word on technical standards. AI standards when issued will be a boon for AI customers seeking assurance that the AI systems they procure will meet appropriate requirements, much as the ISO/IEC 27000 family of standards has done for information security.

The ISO/IEC and other technical standards bodies are active on AI standardisation. The ISO/IEC JTC (Joint Technical Committee) 1 /SC (Sub-Committee) 42 (on AI)[119] was established in October 2017 and, at the time of writing, has published 15 technical standards including in August 2022 an overview of AI ethical and societal concerns.[120]

Sub-Committee 42 is currently working on 24[121] further standards and related documents, including technical specifications on explainability,[122] bias[123] and quality evaluation.[124]

Organisations should keep abreast of standards development in the AI area so, when tendering for AI technology, they can consider whether prospective providers can give the assurance provided by relevant technical standards.

Table 4: Summary of September 2020 UK Government Data Ethics Framework[125]

Overarching Principles	
Principle 1: Transparency Your actions, processes and data are made open to inspection by publishing information about the project in a complete, open, understandable, easily-accessible, and free format.	
Principle 2: Accountability There are effective governance and oversight mechanisms for any project.	
Principle 3: Fairness You have eliminated your project's potential to have unintended discriminatory effects on individuals and social groups.	
Specific Actions ("SA")	
Specific Action 1: define and understand public benefit and user need. When starting a data project, you must have a clear articulation of its purpose. This includes having clarity on what public benefit the project is trying to achieve.	
SA1.1 – Understand the wider public benefit	**SA1.6** – Understand the user need
SA1.2 – Understand the unintended consequences of	**SA1.7** – Ensure there is a clear articulation of the

[119] See here: <https://tinyurl.com/y676dnu2>.
[120] ISO/IEC TR 24368:2022, available here: <https://tinyurl.com/5b97xvsf>.
[121] Listed at: <https://tinyurl.com/4m747e8u>.
[122] ISO/IEC AWI TS 6254 <https://tinyurl.com/4h5xbpff>.
[123] ISO/IEC AWI TS 12791 <https://tinyurl.com/5aatfa3p>.
[124] ISO/IEC AWI TS 5471 <https://tinyurl.com/2c3e3pay>.
[125] Government Digital Service, *Data Ethics Framework* (September 2020) <https://tinyurl.com/yck4nk7j>.

your project	problem before you start the project
SA1.3 – Human rights considerations	**SA1.8** – Check if everyone in your team understands the user needs and how using data can help
SA1.4 – Justify the benefit for the taxpayers and appropriate use of public resources in your project	**SA1.9** – Repeatedly revisit your use need throughout the project
SA1.5 – Make your user need and public benefit transparent	
Specific Action 2: involve diverse expertise. Diverse, multidisciplinary teams with broad skill sets contribute to the success of our data and tech projects. Where we need additional expertise, we involve others from our team or wider organisation with the right experience.	
SA2.1 – Get the right expertise	**SA2.4** – Effective governance structures with experts
SA2.2 – Ensure diversity within your team	**SA2.5** – Transparency (where appropriate, publish information on expert consultations and project team structure)
SA2.3 – Involve external stakeholders	
Specific Action 3: comply with the law. We understand the laws and codes of practice that relate to our use of data. If in doubt, we consult relevant experts.	
SA3.1 – Get legal advice	**SA3.5** – Transparency (publish DPIA and related documents)
SA3.2 – It is your duty and obligation to obey the law in any data projects. You must ensure the project's compliance with GDPR and DPA 2018	**SA3.6** – Ensure the project's compliance with the Equality Act 2010
SA3.3 – Data protection by design and DPIA	**SA3.7** – Ensure effective governance of your data
SA3.4 – Accountability (what are you doing to document data processing – GDPR Arts. 5(2) and 30?)	**SA3.8** – Ensure your project's compliance with any additional regulations
Specific Action 4: review quality and limitations of data. We recognise our technology is only as good as the data and practices used to create it. We ensure that the data we use is accurate, representative, proportionally used, of good quality, and that we can explain its limitations.	
SA4.1 – Data source (provenance)	**SA4.6** – Make your data open and shareable wherever possible
SA4.2 – Determining proportionality (using the minimum data necessary)	**SA4.7** – Share your models
SA4.3 – Bias in data	**SA4.8** – How to ensure transparency of sensitive models
SA4.4 – Data anonymisation	**SA4.9** – Explainability
SA4.5 – Robust practices (in particular re algorithms)	
Specific Action 5: continuous evaluation. We have a plan to continuously evaluate if insights from data are used responsibly. This involves both development and implementation teams. There is a robust evaluation plan and effective accountability mechanisms.	
SA5.1 – Evaluate the project	**SA5.5** – Accountability structures
SA5.2 – Repeatedly revisit the user need and public benefit throughout the project	**SA5.6** – Public scrutiny
SA5.3 – Check how your project influences policy	**SA5.7** – Share your learnings
SA5.4 – Ensure there are skills, training, maintenance for longevity of the project	

G. CONCLUSION

Conclusion. AI – the combination of very large datasets with machine learning and the other streams of AI technologies – is a central part of the deep digital transformation of the fourth industrial revolution we are now going through. As AI develops, it may come to affect our home and working lives perhaps as much as any industrial change. There are many examples of AI in action across business sectors from legal services to construction and from automotive to healthcare. AI will challenge legal assumptions in the

short, medium and long terms. Policy makers and regulators are consequently grappling with what AI means for law and policy and the necessary technical, legal and regulatory frameworks. The past twelve months have seen important policy announcements across the world, but as the approaches of the EU, US and UK show, there is no clear consensus yet. In order to successfully manage AI projects, lawyers in the field will need to keep up to date with AI related regulatory and policy developments in data protection, contract, intellectual property and tort law as the legislature makes new statute law and the courts decide disputes and make new case law. AI is already another fascinating area for technology lawyers.

Chris Kemp
Kemp IT Law LLP, London
December 2022
chris.kemp@kempitlaw.com
+44 (0)20 3011 1678

Annex 1: Glossary

Acronym	*Term*	*Where first used*
ADS	Automated Driving System	C.20
AEVA	The Automated and Electric Vehicles Act 2018	C.19
AI	Artificial Intelligence	A.1
AIaaS	AI as a Service	C.14
API	Application Programming Interface	C.17
ASDE	Authorised Self-Driving Entity	C.20
AWS	Amazon Web Services	C.14
CAGR	Compound Annual Growth Rate	A.4
CAV	Connected and Autonomous Vehicle	C.19
CDDO	Central Digital and Data Office	F.35
CDEI	Centre for Data Ethics and Innovation	C.20
CDPA	The Copyright Designs and Patents Act 1988	D.23
CLI	Command Line Interface	B.11
CPUs	Central Processing Units	B.9
EDPB	European Data Protection Board	C.20
FCA	Financial Conduct Authority	C.18
GCP	Google Cloud Platform	C.14
GPU	Graphics Processing Unit	A.3
GUI	Graphical User Interface	B.11
IPR	Intellectual Property Rights	D.23
ICO	Information Commissioner's Office	D.25
ISO	International Organization for Standardization	A.2
Lidar	**Li**ght **d**etection **a**nd **r**anging	C.19
LPO	Legal Process Outsourcer	C.17
LSA	Legal Services Act 2007	C.18
LSB	Legal Services Board	C.18
LSP	Legal Services Provider	C.18
NLP	Natural Language Processing	A.3
OECD	Organization for Economic Co-operation and Development	A.2
OSS	Open-source Software	F.36
OSTP	White House Office of Science and Technology Policy	E.33
PA	Patents Act 1977	D.23
PRA	Prudential Regulation Authority	C.18
Radar	**Ra**dio **d**etection **a**nd **r**anging	C.19
SCCF	SRA Code of Conduct for Firms	C.18
SCCS	SRA Code of Conduct for Solicitors, RELs and RFLs	C.18
SOA	Services-Oriented Architecture	C.14
SRA	Solicitors Regulation Authority	C.18
TTS	Text-to-Speech	B.11
UIC	User In Charge	C.20
UK IPO	UK Intellectual Property Office	D.23

KEMP IT LAW

Tech Law at the Apex

Chris Kemp
Partner

T: 020 3011 1678
M: 07710 396 071
chris.kemp@kempitlaw.com