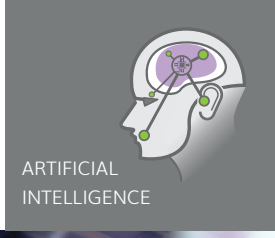
KEMP IT LAW

IT Law at the Apex



White Paper

Legal Aspects of Artificial Intelligence (v. 3.0)

Chris Kemp

February 2021

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE
TABLE OF CONTENTS

FIGURES, TABLES AND ANNEXES

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE (v. 3.0)[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 extent of the current pace of change in artificial intelligence ("**AI**"). The amount of computer processing power (often called 'compute') required to train the most complex algorithms now doubles every 3.5 months. Between 2012 and 2018, the compute requirements of the most demanding models increased 300,000-fold[2] and by mid-2019 it was estimated that the costs – in terms of compute and electricity – of training a single complex algorithm could exceed $3m.[3] This 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. **The impact of COVID-19.** The COVID-19 pandemic has added new dimensions to AI's development. It has both increased the rate of AI adoption and broadened its use cases. This presents new opportunities and new risks. On the one hand, AI offers new ways of fighting the pandemic. As one of many examples, NHS[X], the UK NHS's digital transformation unit, has recently made the National COVID-19 Chest Imaging Database ("**NCCID**") available to researchers to develop AI tools to improve the treatment of COVID-19 patients.[5] On the other hand, the rapid deployment of AI technologies in sensitive areas like healthcare creates obvious challenges. A recent paper in the *BMJ* examining a number of AI-powered COVID-19 prediction models illustrates the point:

   > "prediction models for COVID-19 are quickly entering the academic literature to support medical decision making at a time when they are urgently needed. [The paper] indicates that almost all published prediction models are poorly reported, and at high risk of bias such that their reported predictive performance is probably optimistic… unreliable predictions could cause more harm than benefit in guiding clinical decisions."[6]

   This background of opportunities and risks goes to the heart of the emerging legal and regulatory framework for AI.

3. **What is 'Artificial Intelligence'?** 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.[7]

---

[1] The main changes in v3.0 are: (i) updates to **Section D** (Legal Aspects of AI) (in particular Section **D.21** (AI and Data Protection)) and (ii) the addition of a standalone section on AI Regulation (**Section E**). All websites referred to were accessed in February 2021.

[2] 'The cost of training machines is becoming a problem', *The Economist* (11 June 2020) <Computing hardware - The cost of training machines is becoming a problem | Technology Quarterly | The Economist>.

[3] Emma Strubell et al., 'Energy and Policy Considerations for Deep Learning in NLP', College of Information and Computer Sciences, University of Massachusetts, Amherst (2019) <[1906.02243] Energy and Policy Considerations for Deep Learning in NLP (arxiv.org)>.

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

[5] Department of Health and Social Care, *AI at the forefront of efforts to treat coronavirus patients* (17 January 2021) <AI at the forefront of efforts to treat coronavirus patients - GOV.UK (www.gov.uk)>.

[6] Various authors, 'Prediction models for diagnosis and prognosis of COVID-19: systematic review and critical appraisal', *BMJ* (12 January 2021) <Prediction models for diagnosis and prognosis of covid-19: systematic review and critical appraisal | The BMJ>.

[7] Alan Turing, 'Computing Machinery and Intelligence', *Mind* (October 1950) <I.—COMPUTING MACHINERY AND INTELLIGENCE | Mind | Oxford Academic (oup.com)>, pp. 433-460.

Textbook definitions vary. One breaks the definition down into two steps, addressing machine intelligence and then the qualities of intelligence:

> "artificial intelligence is that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment."[8]

In 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."[9]

More recently, in its January 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."[10]

4. **The technical context.** Since the early years of AI in the 1950s, AI has progressed unevenly. The last decade however has seen rapid progress, driven by growth in data volumes, the rise of the cloud, the refinement of graphics processing units ("**GPUs**") and the development of AI algorithms. This has led to the emergence of a number of separate, related AI technology streams – machine learning, natural language processing ("**NLP"**), expert systems, vision, speech, planning and robotics (see **Figure 2** para **B.9** below).

   Although much AI 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').

5. **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 consultancy IDC predicts that global spending on AI will more than double from $50bn in 2020 to $110bn in 2024. IDC forecasts that the leading drivers for enterprise AI adoption are improving customer experience and enhancing employee performance. This, IDC notes, is reflected in the four leading use cases for AI: automated customer service agents, sales process recommendation and automation, automated threat intelligence and prevention, and IT automation. Together, these four use cases represented nearly a third of AI spending in 2020.[11]

6. **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 what it does, 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

[8] Nils Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (Cambridge: CUP, 2010) <The Quest for Artificial Intelligence (stanford.edu)>, p. 13.
[9] ISO/IEC 2392:2015, definition 2123770 <ISO/IEC 2382:2015(en), Information technology — Vocabulary>. (ISO/IEC 2392:2015 is the ISO/IEC's core IT vocabulary standard.)
[10] Microsoft, *The Future Computed: Artificial Intelligence and its Role in Society* (2018) <The-Future-Computed.pdf (microsoft.com)>.
[11] IDC, *Worldwide Spending on Artificial Intelligence is Expected to Double in Four Years, Reaching $110 Billion in 2024* (25 August 2020) <Worldwide Spending on Artificial Intelligence Is Expected to Double in Four Years, Reaching $110 Billion in 2024, According to New IDC Spending Guide>.

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 AI ethics principles (around fairness, safety, reliability, privacy, security, inclusiveness, accountability and 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 data protection, intellectual property and negligence – and sector specific regulation – in areas of business like healthcare, transport and financial services – will evolve to meet the new requirements.

These rapid developments are leading governments and policymakers around the world to grapple with what AI means for law, policy and regulation and the necessary technical and legal frameworks.

7. **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** two 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 legal services (**C.15** and **C.16**) and connected and autonomous vehicles (**C.17** and **C.18**);
- reviews at **Section D** the legal aspects of AI from the standpoints of data protection (**D.21**), agency law (**D.22**), contract law (**D.23**), intellectual property law (**D.24** and **D.25**) and tort law (**D.26**);
- considers at **Section E** regulatory and policy development across three jurisdictions: the EU (**E.28**), the US (**E.29**) and the UK (**E.32**); 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 15 February 2021 and from the perspective of English law.

B. THE TECHNOLOGIES AND STREAMS OF AI

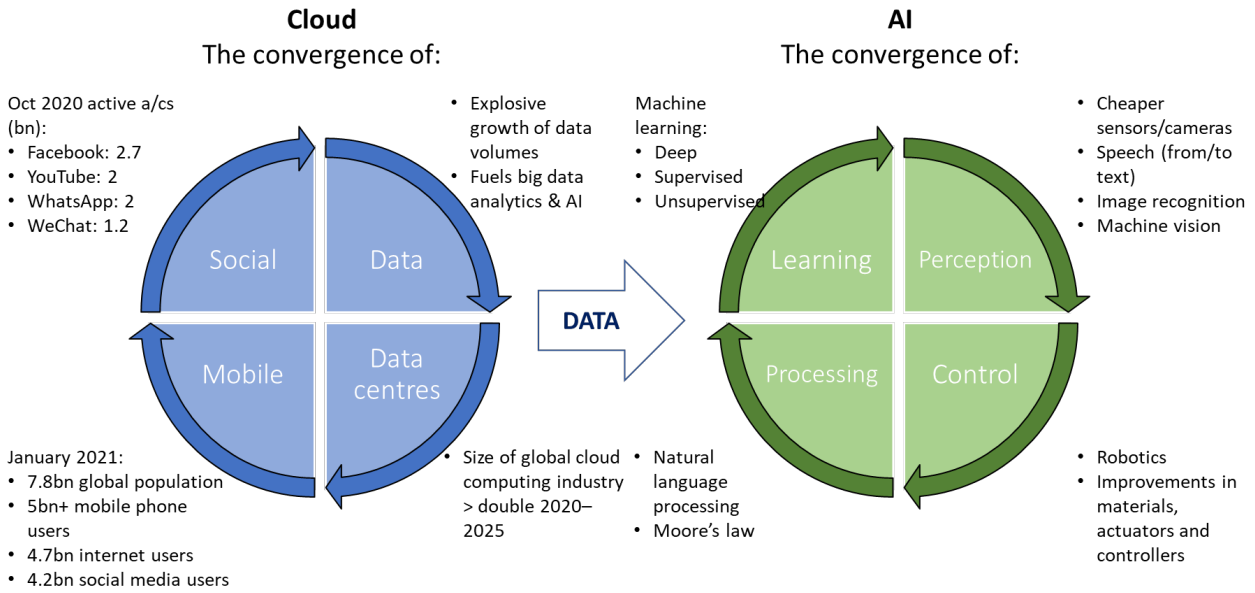
8. **The cloud and AI as twinned convergences: importance of the cloud.** Developments in AI have been fuelled by the ability to harness huge tides of digital data. The vast volumes of varied data arriving at velocity are a product of the cloud, shown in **Figure 1** below as the convergence of data centres, the internet, mobile, and social media. Data centres – increasingly in the form of huge "hyperscale" sites[12] – 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 doubling of the size of the global cloud computing industry to c.$830bn in the five years to 2025.[13]

[12] 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 as marketing term as a classification type. The largest operators (Google, Microsoft, Amazon Web Services, etc.) are increasingly referred to as operating at "mega hyperscale".

[13] ResearchandMarkets.com, *Cloud Computing Market by Service Model, Deployment Model, Organization Size, Vertical and Region – Global Forecast to 2025* (August 2020) <Cloud Computing Market by Service Model (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), Deployment Model (Public and Private), Organization Size, Vertical, and Region - Global Forecast to 2025 (researchandmarkets.com)>.

Internet, mobile and social media use at scale are in turn driving the cloud. The COVID-19 pandemic has only increased the rate of change: during the global "stay at home" period between February and April 2020, total internet traffic grew by almost 40%. For a global population of 7.8bn in early 2021, there are currently estimated to be more than 5.2bn unique mobile phone users, 4.7bn internet users and 4.2bn active social media users. Increasing internet, mobile and social media use is in turn fuelling an explosion in digital data volumes. Research suggests that 1.7MB of data is created for every person on earth every second. This equates to 500hrs of new YouTube content uploaded, 404,000 hours of Netflix video streamed, and 41m WhatsApp messages sent, every minute.[14] It is the availability of data at this scale that provides the raw material for AI.

Figure 1: Twinned convergences: the cloud and AI



9. **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 (para **B.10** below), learning (**B.11**), perception (**B.12**) and control (**B.13**). In the words of Jerry Kaplan in *Humans Need not Apply*, what has made AI possible is:

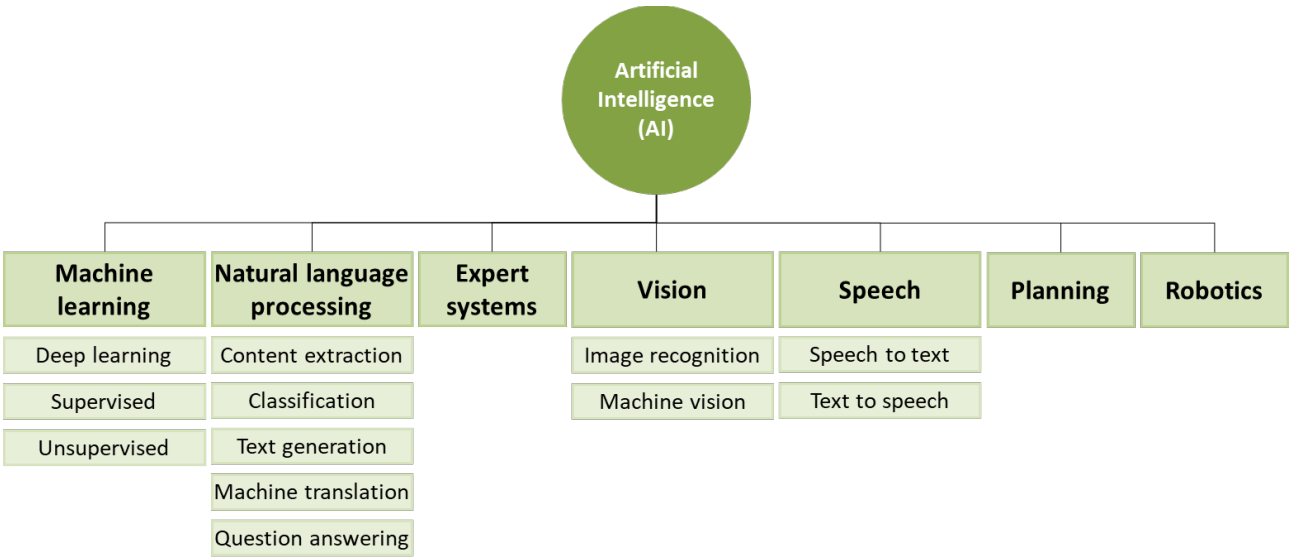
   > "the confluence of four advancing technologies… vast increases in computing power and progress in machine learning techniques… breakthroughs in the field of machine perception… [and] improvements in the industrial design of robots."[15]

[14] Sources: (i) internet traffic: Sandvine Corporation, *The Global Internet Phenomena Report COVID-19 Spotlight* (7 May 2020) <COVID Internet Phenomena Report 20200507.pdf (sandvine.com)>; (ii) global population: Worldometer.info <World Population Clock: 7.8 Billion People (2021) - Worldometer (worldometers.info)>; (iii) mobile, internet and social media users: Datareportal.com, *Digital 2021: Global Overview Report* (27 January 2021) <Digital 2021: Global Overview Report — DataReportal – Global Digital Insights>; (iv) data per second: Domo, *Data Never Sleeps 6.0* (June 2018) <Data Never Sleeps 6 | Domo>; and (v) YouTube, Netflix and WhatsApp: Domo, *Data Never Sleeps 8.0* (August 2020) <Data Never Sleeps 8.0 Infographic | Domo>.

[15] 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.

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 areas of machine capability.

Figure 2: The main AI streams



10. **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 at the moment.

    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.

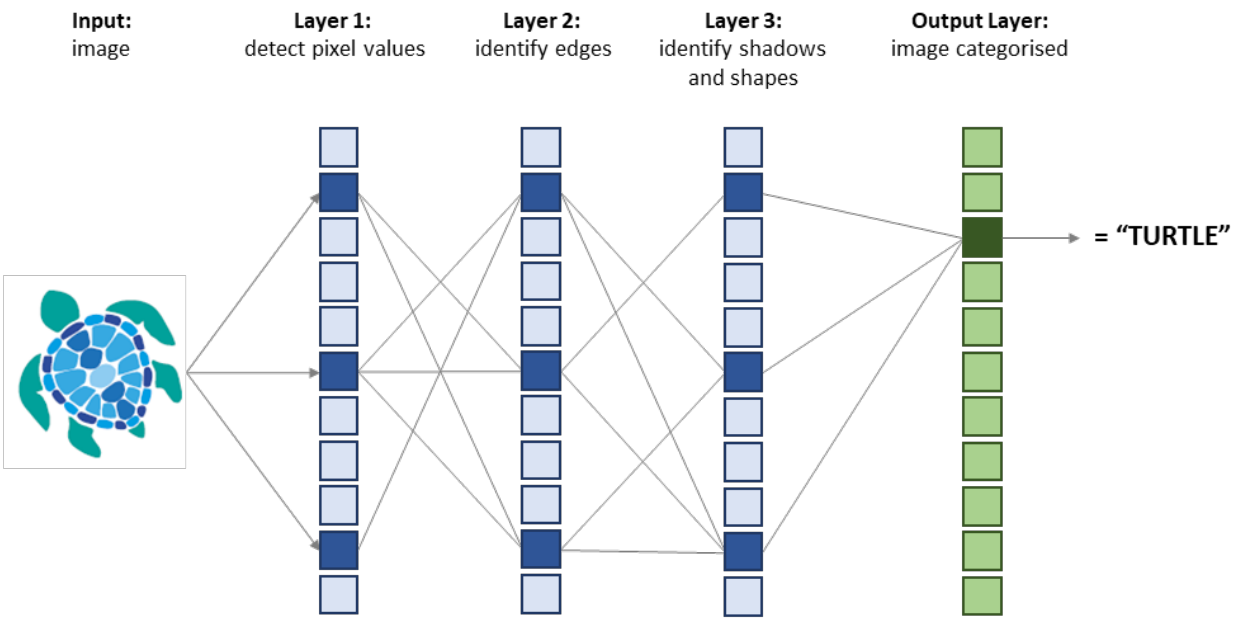
11. **Machine learning: modalities – deep, supervised and unsupervised.** Exponential growth in computer processing power has enabled the development of the streams of machine learning – deep learning, supervised learning and unsupervised learning – by which computers learn by example or being set goals 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 from images, sounds 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 neurons, are inspired by the structure of the human brain.[16] For example, a computer may teach itself to recognise the image of a turtle by breaking the input data down into pixels and then into layers, where information analysing the problem is passed from layer to layer of increasing abstraction and then

[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.

combined in stages until the final output layer can categorise the entire image. How this process works is shown in **Figure 3**.

Figure 3: Neurons and networks [17]



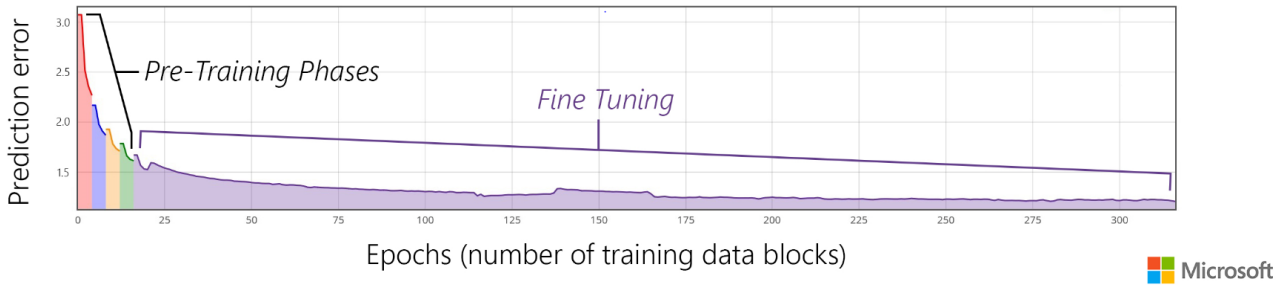
Neural networks work in layers. (1) The computer's memory presents an input to the network – a pixelated image of a turtle. (2) Data from a pixel in the Input causes a neuron in Layer 1 (a square in the graphic) to signal its analysis to neurons in Layer 2, and so on. (3) Each layer analyses a particular 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 connected neurons. Once trained, fine tuning decreases the error rate and increases the accuracy of predictions. To show how this happens, Microsoft provided in a 2016 blog[18] an example of how the Microsoft Cognitive Toolkit used training sets to increase training speech recognition accuracy. This is reproduced at **Figure 4** below.

Deep learning is emerging as AI's "killer app" enabler, and this approach – using the 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[19] including law (standardisable componentry of repeatable legal tasks), accountancy (auditing and tax), insurance (coupled with IoT sensors) and autonomous vehicles.

[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), <AI in the UK: ready, willing and able (parliament.uk)>, p. 21.
[18] Microsoft Blog, *Microsoft releases beta of Microsoft Cognitive Toolkit for deep learning advances* (25 October 2016) <Microsoft Cognitive Toolkit beta released for deep learning advances>.
[19] 'Artificial Intelligence – The Return of the Machinery Question', *The Economist* (25 June 2016) <Artificial intelligence - The return of the machinery question | Special report | The Economist>.

Figure 4: Microsoft Cognitive Toolkit: epochs of training set use increase speech recognition accuracy



Supervised learning is the most common type of machine learning. 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 then 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.

12. **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 images, sound, text, unstructured data or in combination) and "see", "hear", "listen", "comprehend", "speak" and "reason".

    Natural language processing is emerging as a primary human 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. It has been reported that 27% of the online population uses voice mobile voice search.[20] Microsoft's Bing translator enables web pages and larger amounts of text to be translated increasingly accurately in real time.

    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. In late 2020, Microsoft's Azure AI image captioning applications were able to create captions that were more descriptive and accurate then captions for the same images written by humans.[21]

[20] Google, *Think with Google* <Voice search mobile use statistics - Think with Google>.
[21] Microsoft Blog, 'What's that? Microsoft's latest breakthrough, now in Azure AI, describes images as well as people do' (14 October 2020) <What's that? Microsoft's latest breakthrough, now in Azure AI, describes images as well as people do - The AI Blog>.

Machine perception is also developing quickly in ***speech***, where accuracy has met or exceeded that of professional human transcribers for some years now.[22] A notable trend here is the recent push into speech-based AI services by organisations whose roots lie outside AI-enabled tech. A good example is the BBC's 'Beeb' voice assistant, a Beta-GA version of which was released in November 2020.[23]

13. **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 increasing use of different types of robots. In 2019, c.2.7m industrial robots were in operation in the world's factories, up 66% from 2015 (1.6m), although the impact of COVID-19 is expected to have dented the 2020 figures.[24] Global units of domestic consumer robots shipped are forecast to triple from 9m units to 29.6m units between 2018 and 2025.[25]

C. AI IN PRACTICE: CASE STUDIES

14. **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 works through two case studies, highlighting in each case background market and technology developments and then reviewing legal and regulatory aspects:

    - AI in legal services as "static AI" (paras **C.15** and **C.16**); and
    - connected and autonomous vehicles as "mobile AI" (**C.17** and **C.18**).

    Case study 1: AI in legal services

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

    Background: AI and the legal services market. The legal services sector is a £35bn industry in the UK accounting for around 2% of GDP.[26] It is representative of UK professional and business services generally, which together account for £190bn or 11% of UK GDPR.

    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;

[22] Since August 2017, in Microsoft's case: see Microsoft Blog, 'Microsoft researchers achieve new conversational speech recognition milestone' (20 August 2017) <Microsoft researchers achieve new conversational speech recognition milestone - Microsoft Research>.
[23] Microsoft Blog, 'Beeb, how do you build the world's first public service voice assistant?' (25 November 2020) <Beeb, how do you build the world's first public service voice assistant? (microsoft.com)>.
[24] International Federation of Robotics, IFR Press Conference slide deck (24 September 2020) <PowerPoint-Präsentation (ifr.org)>.
[25] Statista, *Unit shipments of domestic consumer robots worldwide from 2015 to 2025 (in millions)* <Global domestic robot shipments 2015-2025 | Statista>.
[26] (2018 figures) Legal services: Competition & Markets Authority, *Review of the Legal Services Market Study in England and Wales* (2020) <Review of the legal services market study in England and Wales - GOV.UK (www.gov.uk)>, p. 14. UK GDP: Office for National Statistics, *Gross Domestic Product: chained volume measures: Seasonally adjusted £m* <Gross Domestic Product: chained volume measures: Seasonally adjusted £m - Office for National Statistics (ons.gov.uk)>.

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.[27] The 2020s are predicted to be the decade of AI systems in the professions.[28]

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 95,000 in 2019. The rate of growth of UK in-house solicitors is even more dramatic, increasing by around sixteen times from 2,000 in 1990 to just over 33,000 in 2019. The ratio of in-house to private practice solicitors in the UK now stands at almost 1:4, up from 1:20 in 1990.[29]

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).

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. Many large firms have now partnered with specialist AI providers like Kira, Luminance and ThoughtRiver to innovate in these areas. Other buyers of legal services have looked to develop in-house solutions: JPMorgan's contract review platform, COIN, is said to save 360,000 hours of lawyers' time annually.[30] Lawtech corporate activity continues to be active, with Thomson Reuters acquiring datasite and workflow management company HighQ (July 2019).

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, 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

[27] 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.
[28] See further Richard and Daniel Susskind, *The Future of the Professions: How Technology will Transform the Work of Human Experts* (Oxford: OUP, 2015), p. 160.
[29] The Law Society, *Trends in the Solicitors' Profession: Annual Statistics Report 2019* (19 October 2019) <Annual Statistics Report 2019 | The Law Society>.
[30] Hugh Son, '*JPMorgan software does in seconds what took lawyers 360,000 hours*', Independent (28 February 2017) <JPMorgan software does in seconds what took lawyers 360,000 hours | The Independent | The Independent>.

– in-house, law firm, LPO and AI provider – and then seamlessly combined. In M&A due diligence 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".

How quickly will AI arrive? AI is proving somewhat challenging at the moment and there are several hurdles to overcome, including structuring and labelling datasets correctly, deciding on the right number of training iterations to balance accuracy and risk, and cultural inhibitors to adoption. On the in-house side, two recent surveys have found that although law departments do not underestimate AI's potential, they are not currently racing towards adoption. One report found that GCs were cautious about advocating AI without clearly proven operational and efficiency advantages and wanted their law firms to do more.[31] Another survey, of 200 in-house lawyers, found that the main hurdles to AI adoption in-house were cost, reliability and appetite for change:[32] this survey's authors concluded that AI in-house was set for a "long arc of adoption" because "it will be difficult to sell AI to the current and next generation of GCs." Only 20% of respondents thought that AI would be in the mainstream in the next five years, 40% said it would take ten years, and the remaining 40% thought it would take even longer.

16. **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[33] so that most "legal activities"[34] are unregulated.[35] The Legal Services Board ("**LSB**") oversees the regulation of lawyers and has appointed eight approved regulators, of which the Solicitors Regulation Authority ("**SRA**") is the primary regulator of solicitors.[36]

Indirect regulation. In addition to direct regulation, law firms and other legal services providers ("**LSPs**") may be indirectly regulated by their client's regulator where that client is itself regulated, for example by the

[31] Legal Week, 'General counsel call on law firms to share the benefits of new artificial intelligence technology' (20 September 2017) <General counsel call on law firms to share the benefits of new artificial intelligence technology | Law.com International>.
[32] Thomson Reuters, 'Legal Department 2025: Ready or Not: Artificial Intelligence and Corporate Legal Departments' <https://static.legalsolutions.thomsonreuters.com/static/pdf/S045344_final.pdf>.
[33] 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.
[34] 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.
[35] Contrast the position in the USA for example, where the US State Bar Associations much more zealously protect against the unauthorised practice of law.
[36] 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.

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 contract 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.[37] 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[38] and parts of the SRA Codes of Conduct that apply generally.

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**")[39] and second, the Code of Conduct for Firms ("**SCCF**").[40] Unlike the predecessor SRA Code of Conduct[41], 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 services (whether third party or proprietary) is an obligation to remain accountable and a requirement to take a risk-based approach.

The requirements of the SCCS are similar, though tailored to individuals: **SCCS 3.5** requires individuals, when supervising or managing others providing legal services to "remain accountable for the work carried out through them" and to "effectively supervise work being done for clients." **SCCS 8.6** introduces a requirement to ensure clients "are in a position to make informed decisions about the services they need, how their matter will be handled and the options available to them."

In both the SCCF and the SCCS (at **6.3** in each) confidentiality is also highlighted: "you keep the affairs of current and former clients confidential unless disclosure is required or permitted by law or the client consents."

Although no longer in effect and replaced by the November 2019 documents, the specific outsourcing-related provisions of the SRA Handbook[42] are still relevant as an indicator of good practice. In the

[37] Available at: <SRA | SRA Standards and Regulations | Solicitors Regulation Authority>.
[38] Available at: <SRA | Principles | Solicitors Regulation Authority>. 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.
[39] Available here: <SRA | Code of Conduct for Solicitors, RELs and RFLs | Solicitors Regulation Authority>.
[40] Available here: <SRA | Code of Conduct for Firms | Solicitors Regulation Authority>.
[41] An archive copy of which is available here: <SRA | Code of Conduct | Solicitors Regulation Authority>.
[42] Available here: <SRA | SRA Handbook | Solicitors Regulation Authority>.

introduction to Chapter 7 of the (old) SRA Code of Conduct, "outsourcing" is described as "using a third party to provide services that you could provide". Under outcome 7.10, the (old) SRA Code of Conduct required a firm carrying out outsourcing to ensure that the outsourcing: (i) does not adversely affect compliance; (ii) does not alter its obligations to clients; (iii) is subject to the contractual arrangements enabling the SRA or its agents to "obtain information from, inspect the records… of, or enter the premises of, the third party" provider.

Client engagement terms: LSPs. LSPs using AI in client service delivery should consider using express terms around AI use in their client engagement arrangements to set appropriate expectations for service levels and standards consistently with SRA duties. SRA regulated LSPs if seeking to limit liability above the minimum[43] 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 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 2: connected and autonomous vehicles ("CAVs")

17. **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. In January 2021, UK Government transport and CAV innovation agency Connected Places Catapult estimated that the global CAV market would be worth £17bn by 2025. By 2035 Connected Places Catapult's base projection is that this will have risen to £650bn, 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 (76.4%), followed by vans (20.1%) and then HGVs and busses (3.4%). 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.[44]

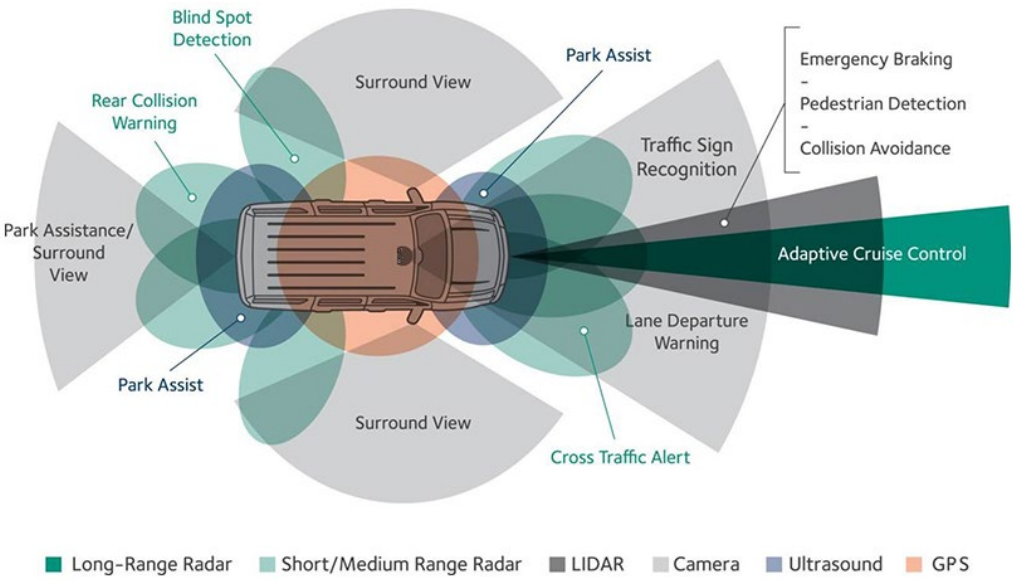
"Vehicles", "connectedness" and "autonomy".[45] By "**vehicles**" we mean passenger cars and commercial vehicles, although AI of course will affect other types of vehicles as well as rail, sea, air and space transportation. "**Connected**" means that the vehicle is connected to the outside world, generally 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. "**Autonomous**" means that the vehicle itself is

[43] LSPs must hold an "appropriate level" of PII (**O(7.13)**) which under the Insurance Indemnity Rules 2012 must not be less than £3m for Alternative Business Structures, limited liability partnerships and limited companies and £2m in all other cases.
[44] All figures from Connected Places Catapult, *Market Forecast for Connected and Autonomous Vehicles* (January 2021) <Connected Places Catapult market forecast for connected and autonomous vehicles (publishing.service.gov.uk)>.
[45] For an excellent guide see Harry Surden and Mary-Anne Williams, 'Technological Opacity, Predictability, and Self-Driving Cars', *Cardozo Law Review* 38 (2016) <Technological Opacity, Predictability, and Self-Driving Cars by Harry Surden, Mary-Anne Williams :: SSRN> pp. 121-181.

capable with little or no human intervention of making decisions about all its activities: steering, accelerating, braking, lane positioning, routing, complying with traffic signals and general traffic rules, and negotiating the environment and other users. So a vehicle may be connected without being autonomous, but cannot be autonomous without being connected.

Sensors, digital maps and the central computer. To act autonomously in this way, the vehicle 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 and in real time by means of sensors, digital maps and a central computer. **Figure 5** below shows the types of onboard sensors that an autonomous vehicle uses to gather information about its environment, including short, medium and long-range radar (**ra**dio **d**etection **a**nd **r**anging), lidar (**li**ght **d**etection **a**nd **r**anging – essentially laser-based radar to build 3D maps), cameras and ultrasound.

Figure 5: CAVs' on board sensors[46]



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 dynamically 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 times 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

[46] Image adapted from <Autonomous Vehicles | NovAtel>.

representation to the digital map. In the ***acting*** phase, the computer moves the vehicle by activating its driving systems.

18. **CAVs: regulatory aspects**

Towards CAV regulation: issues to be addressed. Since the first of the UK Locomotive ('Red Flag'[47]) 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 CAVs predicate will therefore transform over 150 years of national and international vehicle, road and traffic legislation and regulation. Key regulatory issues that must be resolved for road authorisation of CAVs include: (i) connectivity from the vehicle's sensors to other vehicles, objects, road and traffic infrastructure and the environment; (ii) the digital representation of the physical world that the vehicle interacts with; (iii) the computer's system for decision making and control; (iv) roadworthiness testing; and (v) relevant human factors.

SAE International's six levels of driving automation. SAE International, a standards body, has mapped[48] six levels of driving automation to four modes of dynamic driving tasks, as summarised in **Table 1** below.

Table 1: CAVs – Four modes of driving and six levels of automation

Six Levels of Driving Automation	Four Modes of Dynamic Driving Tasks			
	1 Controlling speed and steering	2 Monitoring driving environment	3 'Fallback' (failover) performance	4 Human or system control of driving
1 None				
2 Driver assistance				
3 Partial				
4 Conditional				
5 High				
6 Full				

For the first three levels (no automation, driver assistance and partial automation), the human driver carries out, monitors and is the fallback for each of the driving modes, with limited automation and system capability for some steering and speed tasks only (like park assist, lane keeping assist and adaptive cruise control). For the second three levels (conditional, high and full automation) the vehicle progressively takes over steering and speed, driving monitoring, fallback performance, and then some – and finally all – driving modes. The UK Department for Transport ("**DfT**") has conveniently summarised these six levels as moving progressively from (human) "hands on, eyes on" through "hands temporarily off, eyes on" to "hands off, eyes off".

The UK's approach to regulation: "the pathway to driverless cars". The DfT has been active in reviewing and preparing for the changes in regulation that will be necessary for CAVs. In 2015 it set up the Centre for

[47] 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).
[48] SAE International Standard J3016_201806, *Taxonomy and Definitions for Terms Related to Driving Automation systems for On-Road Motor Vehicles* (15 June 2018) <J3016B: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International>.

Connected and Autonomous Vehicles ("**CCAV**"), an expert unit tasked with overseeing the UK's regulatory response to CAVs under the general approach the "Pathway to Driverless Cars".

At this early stage, a key focus of the CCAV has been to develop a "light touch/non-regulatory approach" to the testing and development of CAV technologies.[49] In February 2019, the DfT/CCAV published a revised version of its "Code of Practice: Automated vehicle trialling" guidance which emphasises that organisations running CAV trials may do so on roads in the UK without obtaining regulatory permits or paying surety bonds.[50] In February 2020 the British Standards Institution ("**BSI**"), working in conjunction with the CCAV, published PAS 1881: 2020, a document setting out good practice guidance for developing safety cases for CAV trialling.[51]

Looking ahead, a key feature of the regulatory landscape will be the conclusion, and then steps taken to implement, the English and Scottish Law Commissions' ("**LC**") three-year review into the legal framework for CAVs, which is due to provide its final report and recommendations in Q4 2021. The review is now two thirds through. In February 2019, the LC published the results of its first consultation, which considered fundamental safety issues and the approach to criminal and civil liability.[52] In February 2020, the LC completed its second consultation, which focussed on a new concept of Highly Automated Road Passenger Services ("**HARPS**") – services where highly automated vehicles supply road journeys to passengers without a human driver or user-in-charge.[53] The third and final consultation, published in December 2020, focuses on the definition of self-driving and assuring safety in use.[54]

A key challenge for policy makers is that they are aiming at a moving target – regulatory change needs to start now, at a time when it is difficult to predict the future course of CAV development. The UK has therefore decided to take a step-by-step approach, laying the groundwork for future developments with a permissive trialling regime while setting the scene for more fundamental regulatory change over the longer term through the work of the LC. Related changes are also being made to consumer-facing road and vehicle legislation, in both an incremental way – such as amening the Highway Code to permit remote control parking (June 2018)[55], and at a structural level – such as addressing the rules for domestic CAV insurance (July 2018).[56]

CAVs and data protection. The data protection analysis of CAVs presents complex questions. CAVs include a broad range of onboard devices that originate data. By some estimates they can produce up to 25GB of data per hour, most of which is personal data.[57] These devices include GPS, Inertial Measurement Units ("**IMU**"), accelerometers, gyroscopes, magnetometers, microphones (and as shown at **Figure 5** above) radar, lidar, cameras and ultrasound. Data from these originating devices may be used on board, and communicated

[49] DfT, *The Pathway to Driverless Cars: Summary report and Action Plan* (February 2015) <The Pathway to Driverless Cars Summary report and action plan (publishing.service.gov.uk)>, p. 11.
[50] DfT/CCAV, *Code of Practice: Automated vehicle trialling* (February 2019) <Code of Practice: Automated vehicle trialling - GOV.UK (www.gov.uk)>.
[51] BSI , *PAS 1881: 2020 Assuring the Safety of Automated Vehicle Trials and Testing – Specification* <PAS 1881 | BSI (bsigroup.com)>.
[52] See the LC's first consultation paper (here) and a summary of the responses (here).
[53] See the LC's second consultation paper (here) and a summary of the responses (here).
[54] See the LC's third consultation paper (here).
[55] DfT, *'New laws pave way for remote control parking in the UK – From June 2018 drivers will be able to use remote control parking on British roads'* (17 May 2018) <New laws pave way for remote control parking in the UK - GOV.UK (www.gov.uk)>.
[56] The Automated and Electric Vehicles Act 2018 ("**AEVA**"), Part I, ss. 1-9, makes changes to the UK's compulsory motor vehicle insurance regime to enable CAVs to be insured like conventional vehicles. Part 2 makes changes to the UK's electric vehicle charging infrastructure.
[57] European Data Protection Supervisor, *'TechDispatch #3: Connected Cars'* (20 December 2019) <TechDispatch #3: Connected Cars | European Data Protection Supervisor (europa.eu)>.

externally with a number of parties and then further stored and processed. In its September 2016 response to the CCAV's *Pathway to Driverless Cars* consultation, the UK Information Commissioner's Office ("**ICO**") stated:

> "it is likely that data generated by the devices will be personal data for the purposes of the DPA [and] that the collection, storage, transmission, analysis and other processing of the data [the devices] generate will be subject to data protection law".[58]

In January 2020, the European Data Protection Board ("**EDPB**") published guidance on the data processing aspects of CAVs in which it articulated the following privacy and data protection 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.[59] 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.

CAVs and cyber security. Cyber security has also emerged as a critical area of CAV regulation. On 6 August 2017, the UK Government published a set of eight key CAV cyber security principles, focusing on system security ((i) board level governance of organisational security; (ii) appropriate and proportionate assessment of security, (iii) product aftercare) and system design ((iv) organisational collaboration; (v) system defence in depth; (vi) secure management of software throughout its life; (vii) secure data storage/transmission; and (viii) resilience in design).[60]

D. LEGAL ASPECTS OF AI

19. **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.20**). AI is then briefly considered in relation to the law of data protection (**D.21**), agency (**D.22**), contract (**D.23**), intellectual property rights for software (**D.24**) and data (**D.25**), and tort (**D.26**). Regulation of AI is discussed in **Section E**.

20. **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 tools 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

[58] ICO, *Response to the CCAV's consultation "Pathway to Driverless Cars"* (9 September 2016) <dft-pathway-to-driverless-cars-ico-response-20160909.pdf>.
[59] EDPB, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (28 January 2020) <edpb_guidelines_202001_connectedvehicles.pdf (europa.eu)>.
[60] DfT, *Key principles of vehicle cyber security for connected and autonomous vehicles* (6 August 2017) <The key principles of vehicle cyber security for connected and automated vehicles - GOV.UK (www.gov.uk)>.
[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".

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). 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 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 – for example if the views expressed by the European Parliament in 2017 are taken forward.[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.

21. **AI and data protection**

General applicability of the UK GDPR[63] to AI. UK GDPR applies to personal data used in AI. As a "technologically neutral"[64] piece of legislation, it does not contain special AI rules. Instead, UK GDPR's principles-based approach applies to AI just as it does to any other in-scope processing of personal data. As the Information Commissioner wrote in her foreword to the ICO's July 2020 "Guidance on AI and data protection", a useful point to bear in mind from the outset is that:

> "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?"[65]

Having said this, the ICO has also expressed the view that certain features of AI "have implications for data protection and privacy" which "distinguish it from more traditional processing". In particular, the ICO highlights 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.[66]

---

[62] On 16 February 2017 the European Parliament adopted a resolution making recommendations to the Commission on civil law rules on robotics <Texts adopted - Civil Law Rules on Robotics - Thursday, 16 February 2017 (europa.eu)>. 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 <Artificial intelligence: Commission outlines a European approach to boost investment and set ethical guidelines (europa.eu)>.

[63] 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 <Data protection law - GOV.UK (www.gov.uk)>).

[64] UK GDPR, Recital 15. Briefly, on the status of EU GDPR's recitals as an aid to interpreting UK GDPR from 1 January 2021: "Recitals will continue to be interpreted as they were prior to the UK's exit from the EU. They will, as before, be capable of casting light on the interpretation to be given to a legal rule, but they will not themselves have the status of a legal rule" (see 'Explanatory Notes' to the European Union (Withdrawal) Act 2018 <European Union (Withdrawal) Act 2018 - Explanatory Notes (legislation.gov.uk)>, para 83).

[65] Information Commissioner's Office, "Guidance on AI and data protection" <Guidance on AI and data protection | ICO>.

[66] Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection" (September 2017) <big-data-ai-ml-and-data-protection.pdf (ico.org.uk)>, p. 9.

The ICO's AI-specific guidance. The distinctive questions posed by AI to data protection law have led to the publication of several AI-specific guidance documents by the ICO in recent years. The key texts are:

- the "Big data, artificial intelligence, machine learning and data protection" report, first published in 2014 and updated in September 2017;[67]
- the "Explaining decisions made with AI" guidance, a collaboration with the Alan Turing Institute, May 2020;[68] and
- the "Guidance on AI and data protection", July 2020.[69]

These documents form a substantial part of the ICO's response to AI to date and are recommended reading for those looking for an overview of the topic.[70] The remainder of this section is confined to a discussion of the following AI-specific issues for data protection: (i) the AI provider's role as data processor or data controller; (ii) anonymization and other AI data protection compliance tools; (iii) research and pseudonymisation; and (iv) profiling/automated decision-making. These are now briefly considered.

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 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 a 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.

However, the borderline between controller and processor can be fuzzy in practice. The ICO notes that "the definition of a processor can be difficult to apply in the complexity of modern business relationships. In practice, there is a scale of responsibility in how organisations work together to process personal data."[71] [72] This is true in particular for AI, where networks of data can interact with each other in complex and multifaceted ways.

Where the controller/processor borderline lies in the AI context was considered for the first time in the UK in the ICO's July 2017 decision on an agreement between the Royal Free Hospital and Google DeepMind.[73] Under the agreement DeepMind used the UK's standard, publicly available acute kidney injury ("**AKI**") algorithm to process personal data of 1.6m patients in order to test the clinical safety of Streams, an AKI application that the hospital was developing. The ICO ruled that the hospital had failed to comply with data

[67] Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection".
[68] Information Commissioner's Office, "Explaining decisions made with AI" (May 2020) <Explaining decisions made with AI | ICO>.
[69] Information Commissioner's Office, "Guidance on AI and Data Protection (July 2020) <Guidance on AI and data protection | ICO>.
[70] See also Quentin Tannock and Rob Sumroy, 'Data Protection and Privacy' in *The Law of Artificial Intelligence*, ed. by Matt Hervey and Matthew Lavy (London: Sweet & Maxwell, 2021), pp. 347-419.
[71] Information Commissioner's Office, 'How do you determine whether you are a controller or processor?' at <How do you determine whether you are a controller or processor? | ICO>.
[72] See also European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR (adopted on 02 September 2020) <edpb_guidelines_202007_controllerprocessor_en.pdf (europa.eu)>.
[73] Information Commissioner's Office, 'Royal Free – Google DeepMind trial failed to comply with data protection law' (2017) <Royal Free - Google DeepMind trial failed to comply with data protection law | ICO>. See also Julia Powles and Hal Hodson, 'Google DeepMind and Healthcare in an Age of Algorithms', *Health and Technology*, 7(4) (2017) <Google DeepMind and healthcare in an age of algorithms | SpringerLink>, pp. 351-367.

protection law and as part of the remediation required by the ICO, the hospital commissioned law firm Linklaters to audit the system. The hospital published the audit report in May 2018[74], which found (at para 20.7) that the agreement had properly characterized DeepMind as a data processor not a controller and observed (at para 20.6) that Streams:

> "does not use complex artificial intelligence or machine learning to determine when a patient is at risk of AKI (which could suggest sufficient discretion over the means of processing to be a data controller). Instead, it uses a simple algorithm mandated by the NHS."

In suggesting that use of "complex" AI or machine learning to determine an outcome could involve "sufficient discretion over the means of processing" to be a controller, the case raises more questions: is algorithm complexity a relevant criterion in assessing who determines the means of processing? If so, where does the border lie? The controller must determine the "purposes and means" of processing, so if the customer determines the purposes (to find out who is at risk of illness, for example) but the AI provider (and not the customer) determines the means of processing (because the AI algorithm is "complex"), is the provider a controller in that case?

The correct approach to categorising controllers and processors when AI is involved is a developing area. The ICO plan to consult and release further guidance on these questions in 2021, as part of its review of its cloud computing guidance.[75]

AI projects: anonymisation as a compliance tool. As a tool for data protection compliance, anonymisation predates UK GDPR by some distance: the ICO first published its code of practice on anonymisation in November 2012[76] and is working on an update.[77] But the topic received renewed regulatory and public attention in 2020 during the rollout of COVID-19 contact tracing apps – both in Europe and further afield. Regulators focused on anonymisation as a way of protecting individual rights and freedoms in a time of crisis. The EDPB, for instance, issued guidance recommending that developers of contact tracing apps "focus on the use of anonymised location data… rather than personal data".[78] Public debate focused on the difference between the everyday meaning of "anonymisation" and the stricter GDPR requirements, and the attendant privacy implications.[79]

Anonymisation remains a powerful compliance tool because anonymous data is outside the scope of UK GDPR, as it is no longer personal. 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."

---

[74] Linklaters LLP, *Audit of the acute kidney injury detection system known as Streams*' (17 May 2018) <Streams_Report.pdf>.
[75] Information Commissioner's Office, 'What are the accountability and governance implications of AI?' <What are the accountability and governance implications of AI? | ICO>.
[76] Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (November 2012) <Anonymisation: managing data protection risk code of practice (ico.org.uk)>.
[77] Information Commissioner's Office, 'What is personal data?' <What is personal data? | ICO>.
[78] European Data Protection Board, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (adopted on 21 April 2020) <edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (europa.eu)>. See also Open Data Institute, "Anonymising data in times of crisis" (June 2020) <ODI-2020-Anonymising-data-in-times-of-crisis.pdf (theodi.org)>.
[79] See, for example, Matt Burgess, 'Just how anonymous is the NHS Covid-19 contact tracing app?', *Wired* (12 May 2020) <Just how anonymous is the NHS Covid-19 contact tracing app? | WIRED UK>.

The act of anonymising personal data, however, is within scope of UK GDPR (because that processing starts with personal data).[80] UK GDPR does not provide detailed guidance on how far personal data needs to be modified for it to constitute anonymous data. While UK GDPR is generally considered to set a 'high bar', opinion differs on several points, including the ease with which anonymous data can be re-identified as personal data.

For instance, the Article 29 Data Protection Working Party, in an opinion which has not been endorsed by the EDPB, suggests that controllers need to take account "of "all" the means "likely reasonably" to be used for identification by the controller and third parties, paying special attention to… the current state of technology."[81] More recently, Germany's Federal Commissioner for Data Protection and Freedom of Information has proposed a stricter test, arguing that for data to be anonymous, re-identification needs to be "practically impossible".[82]

For the ICO, the risk of re-identification is also the key criterion:

> "Organisations using anonymised data need to be able to show they have robustly assessed the risk of re-identification, and have adopted solutions proportionate to the risk. This may involve a range of technical measures, such as data masking, pseudonymisation and aggregation, as well as legal and organisational safeguards."[83]

For the lawyer advising on anonymisation in the context of an AI project, alerting colleagues to the differences between 'strict' anonymisation on the one hand and 'mere' pseudonymisation on the other (and the UK GDPR implications of this distinction) is key.

AI projects: other compliance tools. The ICO makes five other recommendations for AI in its "Big data, artificial intelligence, machine learning and data protection" report:

- privacy notices: "organisations should be transparent about their processing of personal data… in order to provide meaningful privacy notices";
- data protection impact assessments: "organisations should embed a privacy impact assessment framework into their big data processing activities to help identify privacy risks and assess the necessity and proportionality of a given project";
- privacy by design: "organisations should adopt a privacy by design approach in the development and application of their big data analytics… including implementing technical and organisational measures to address matters including data security, data minimization and data segregation";
- ethical principles: "organisations should develop ethical principles to help reinforce key data protection principles" (See also **Section F** below); and
- auditable machine learning algorithms: "organisations should implement innovative techniques to develop auditable machine learning algorithms [including] internal and external audits… to explain the rationale behind algorithmic decisions and check for bias, discrimination and errors".

---

[80] See Peter Carey, 'Data Protection Principles' in *Data Protection A Practical Guide to UK and EU Law*, fifth edition, ed. by Peter Carey (Oxford: OUP, 2018), pp. 32-42 (39).

[81] Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques" (adopted on 10 April 2014) <xxxx/xx/EN (europa.eu)> , p. 6.

[82] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, "Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche" (29 June 2020). <https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=2>, p. 4.

[83] Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection", p. 61.

AI projects: pseudonymisation as a further compliance tool in research. AI and very large datasets are increasingly being used for data and other scientific research. Personal data processed for scientific research is covered by the UK GDPR (Recital 159) and Art. 89(1) provides that:

> "Processing for… scientific… purposes… shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

Art. 4(5) defines pseudonymisation (caught by UK GDPR by Recital 26) as:

> "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

UK GDPR Recital 28 provides that:

> "The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations."

Pseudonymisation can therefore help as a compliance tool for scientific research, which has certain benefits such as:

- processing for scientific research is considered to be compatible with lawful processing operations (Recital 50 and Art. 6(1)(b));
- the storage limitation principle is somewhat relaxed (Art. 6(1)(e)); and
- the obligations to provide information to data subjects (Recital 52 and Art. 14(5)(b)) and in relation to special categories of data (Recital 65 and Art. 9(2)(j)) are also somewhat wound down.

AI projects: profiling and automated decision making. This area has attracted significant public attention[84] in recent months and the adequacy of existing rules is regularly challenged.[85] For now, 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 automated 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."

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

---

[84] E.g. the 2020 UK GCSE and A-Level grading controversy. See Chris Kemp, 'Please! Save us from your mutant algorithms! An Accountability for Algorithms Act?' (30 October 2020) <SCL: Please! Save us from your mutant algorithms! An Accountability for Algorithms Act?>.

[85] See, e.g. HL Deb 12 February 2020, vol. 801, col. 2333 <Algorithms: Public Sector Decision-making - Wednesday 12 February 2020 - Hansard - UK Parliament>.

"(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."

But by Art. 22(3):

> "In the cases referred to in points (a) and (c) of [Art. 22(2)], the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

Art. 22(4) sets out further restrictions relating to processing of special categories of data referred to at Art. 9(1), including racial/ethnic origin, religious beliefs, genetic, biometric or health data or data about an individual's sex life or sexual orientation.

The Art. 22 right sits on top of the other rights of data subjects and duties of controllers. Establishing the lawful and fair basis of processing and compliance with the other principles thereof remains important, as does adequately noticing the AI activities concerned.

The requirement for decisions to be based "solely" on automated processing and the safeguarding required by Art. 22(3) are leading AI users to consider interposing human evaluation between the machine and the data subject. The tension between UK GDPR's requirements and the costs of human intervention in this way are likely to lead to claims about the quality and genuineness of the human decision making – for the ICO, for example, "the human involvement has to be active and not just a token gesture".[86]

22. **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.20** 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 owner and is possessed by and provided as a licence or a service to the user.

23. **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

[86] Information Commissioner's Office, 'What does the UK GDPR say about automated decision-making and profiling?' at <What does the UK GDPR say about automated decision-making and profiling? | ICO>.

[87] Peter Watts and F.M.B. Reynolds, *Bowstead and Reynolds on Agency*, twenty second edition (London: Sweet & Maxwell, 2021), p. 1.

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.

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 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 "in principle a smart contract can be identified, interpreted and enforced using ordinary and well-established legal principles."[90]

24. **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.[91] A key question 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"

and "computer generated" is defined at s.178 CDPA as meaning:

> "that the work is generated by computer in circumstances such that there is no human author of the

[88] For further information on IT contracts generally see our white paper *Demystifying IT Law* (June 2018) at <http://www.kempitlaw.com/wp-content/uploads/2018/06/Demystifying_IT-White-Paper-KITL-v3.0-June-2018.pdf> and in relation to issues arising in contracting on Digital Transformation projects, our blog *Market Update: Key Digital Transformation Issues in Telecoms, Cloud, Software and Services Contracts*, (October 2020) at <Market Update: Key Digital Transformation Issues in Telecoms, Cloud, Software and Services Contracts – Kemp IT Law>. See also our *Trends in Information Technology Law: Looking ahead to 2021* (January 2021) at <Trends in information technology law: looking ahead to 2021 – Kemp IT Law>.

[89] HG Beale, *Chitty on Contracts*, thirty third edition (London: Sweet & Maxwell, 2020), para 2-148.

[90] UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (November 2019) <Legal statement on cryptoassets and smart contracts (netdna-ssl.com)>.

[91] 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.

work."

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.

AI also poses novel questions for copyright works *input* into an AI system. Works copied in a human brain (e.g. as memories or thoughts) do not infringe copyright. But what happens when a copyright work is copied, stored or used in an AI's "brain"? For example if a neural network AI is trained to recognise the literary influence of Hilary Mantel, using a training dataset consisting of her published works? Even if copyright works are stored in the AI in an abstract form, for instance as a weighting attributed to a neuron in a neural network (se para **B.11**), if the creative elements of a work are reproduced a copy will have been made. In late 2020, the UK Intellectual Property Office ("**UK IPO**") consulted on whether to recommend changes to the UK copyright regime to make it easier for AI to use protected content.[92] At the time of writing, the UK IPO was analysing consultation feedback. For now, if an AI operator is unable to avail itself of an exception to copyright, it will need to have appropriate rights to the input works.

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).[93]

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 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.

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.[94]

---

[92] UK IPO, *Artificial Intelligence Call for Views: Copyright and Related Rights* (7 September 2020) <Artificial intelligence call for views: copyright and related rights - GOV.UK (www.gov.uk)>: "We would like you to consider whether our current exceptions support the AI sector and to what extent exceptions are appropriate for encouraging the use and development of AI. Is there evidence and support for new exceptions, or should we explore other approaches such as increased support for licensing?"

[93] Starting with *Aerotel Ltd v Teloc Holdings Ltd* and *Macrossan's Patent Application* [2006] EWCA Civ 1371.

[94] 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 <Algo IP – Rights in Code: 2020 Update – Kemp IT Law>.

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

What is data? The initial question in respect of the datasets that AI works on is to ask: what is the nature of 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".[95]

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*[96] is generally taken as authority for the proposition that there is no property ***in*** data as it cannot be stolen; and the 2014 *Your Response*[97] 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)[98]. 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 (see **Figure 6** below, *Towards a common legal framework for data*).

---

[95] ISO/IEC Standard 2382:2015, *Information technology – Vocabulary*, terms 2121271 and 2121272. Information and data are used interchangeably here.

[96] [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.

[97] *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.

[98] For a more in-depth review of the technical aspects of data see our *Legal Aspects of Managing Big Data* White Paper (October 2014) and Richard Kemp et al, *Legal Rights in Data* (27 CLSR [2]), pp. 139-151.

Figure 6: 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. 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…"[99]

and the *Your Response* case referred to above that databases cannot give rise to a lien.

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[100]: 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

[99] House of Lords Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?*, HL Paper 100 (April 2018), <AI in the UK: ready, willing and able (parliament.uk)>, p. 28.
[100] CDPA, s. 3(1)(b).

specific to each right, complex and vary from country to country. There is currently also a lively policy 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 powers 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 recently written about the growing importance of trade secrets and database right for AI, algorithms and their related datasets.[101]

26. **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 area 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-enabled or autonomous systems, and the tort of breach of statutory duty may also apply depending on the regulatory backdrop. The UK AEVA 2018 (covered in more detail in **C.17** and **C.18** above), 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.

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"[102], 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?[103]

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 statute 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

[101] See paras E.47 and E.48 of our *Algo IP: Rights in Code – 2020 Update* White Paper (April 2020) < Algo IP – Rights in Code: 2020 Update – Kemp IT Law>.
[102] Lord Macmillan in *Donoghue* v *Stevenson* [1932] A.C. 562 at p. 619.
[103] 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.

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."[104]

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 an aeroplane or a cricket ball driven out of the ground.[105] 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

27. **Introduction.** This section looks at the regulatory and policy landscape for AI across three geographies: first, the EU, which was particularly active in 2020 (**E.28**); second, the US which, in its apparent reluctance to regulate too quickly, is a counterpoint to the EU's approach (**E.29**); and third, the UK, where progress has been made at an institutional level (**E.32**).

28. **The EU: steps toward overarching regulation.**

"Trustworthy, ethical and human-centric AI". In 100 days. The European vision for an overarching "AI Regulation" began to take shape in December 2019 when Commission President Ursula von der Leyen, in her manifesto for the Presidency, made it clear she would "put forward a coordinated European approach on the human and ethical implications of Artificial Intelligence" in her first 100 days in office.[106] This prompted a number of significant documents from Brussels in 2020, including:

- the Commission's "White Paper on Artificial Intelligence", February 2020, which shaped much of the debate in 2020 on AI regulation;
- a subsequent consultation on the Commission's AI White Paper, the results of which were published in July 2020; and
- a "non-paper" from 14 EU Member States warning against overzealous regulation, October 2020.

These documents are now considered briefly.

The Commission's AI White Paper[107] – the "risk-based approach". The Commission's AI White Paper is a tentative, non-binding document which sets out a vision for an EU regulatory framework for AI. The watchword is "trust" (repeated 16 times throughout the document) and the key regulatory idea is a "risk-based approach" which splits AI into "high risk" and "not high risk" categories. The White Paper proposes that AI which is "high risk" should be subject to a set of mandatory requirements.

---

[104] (1866) L.R. 1 Ex. 265 at p. 279.

[105] 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.

[106] Ursula von der Leyen, *A Union that Strives for More: My Agenda for Europe* (9 October 2019) <A Union that strives for more - Publications Office of the EU (europa.eu)>.

[107] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust* (19 February 2020) <commission-white-paper-artificial-intelligence-feb2020_en.pdf (europa.eu)>.

The "high risk" AI test. The White Paper sets out a two-limbed test to determine if an AI application is high risk", with detail on each limb:

- *Limb 1 – Sector.* Is the AI application "employed in a sector where, given the characteristics of the activities typically undertaken, significant risks can be expected to occur"? The White Paper proposes that high risk sectors "should be specifically and exhaustively listed… For instance, healthcare; transport; energy; and parts of the public sector" and that the list should be updated from time to time.
- *Limb 2 – Use.* Is the AI application "used in such a manner that significant risks are likely to arise"? For example, does the use give rise to legal (or similarly significant) consequences for an affected individual or company? Is there a risk of injury, death or significant material or immaterial damage? Does the use produce effects that are unavoidable?

The White Paper is clear that the rules should be proportionate, so the test would be cumulative – both limbs must be met to be high risk. But there could also be "exceptional circumstances" where an AI application could be "high risk" regardless of sectors (e.g. facial recognition) and this would override the test.

Mandatory requirements for "high risk" AI. According to the White Paper, mandatory requirements would only be triggered for AI applications that are "high risk", either because they satisfy the two-limbed test, or because they are otherwise "exceptional". The White Paper is more circumspect about the mandatory requirements themselves – it gives six "key features" (and a few examples) shown in **Table 2** below.

Table 2: the Commission's AI White Paper – Proposed mandatory requirements for "high risk" AI

#	Key Feature	Example
1.	Training data	"Requirements ensuring that AI systems are trained on data sets that are sufficiently broad"
2.	Data and record-keeping	Keep "accurate records regarding the data set used to train and test the AI systems"
3.	Information to be provided	"Citizens should be clearly informed when they are interacting with an AI system and not a human being"
4.	Robustness and accuracy	"Requirements ensuring that outcomes are reproducible"
5.	Human oversight	"Monitoring of the AI system while in operation and the ability to intervene in real time and deactivate"
6.	Specific rules for some AI use cases, e.g. remote biometric identification	N/a

Other aspects 1: conformity assessments. Besides the "high risk" test, which is the key thrust of the White Paper as far as regulation is concerned, two other aspects are discussed. First, a proposed process of "objective prior conformity assessment" to ensure high risk AI applications meet the mandatory requirements. Conformity assessments are a familiar part of EU product legislation: an "ex ante" test to check that a product meets requirements before it is placed on the market. AI conformity assessments could set out procedures for testing, inspecting or certifying AI applications. And they could look further under the bonnet by assessing an AI application's algorithms or training datasets.

Other aspects 2: AI governance framework. Second, the White Paper briefly suggests that the European AI governance framework might consist of "a network of national authorities, as well as sectoral networks and regulatory authorities, at national and EU level". A "committee of experts" – possibly the High Level Expert

Group on AI ("**HLEG**"), an AI advisory body, or an AI equivalent of the European Data Protection Board – "could provide assistance to the Commission".

AI White Paper – consultation feedback. The consultation phase closed in June 2020, by which time it had provoked a significant reaction from businesses and individuals, having attracted over 1,200 responses. The Commission noted a "less straightforward" response to the scope of rules set out in the White Paper, including some considerable disagreement as to whether a new regulation is the right approach. According to the Summary Report on the consultation, "42% of respondents request the introduction of a new regulatory framework on AI, another 33% think the current legislation needs to be modified". Respondents were also ambivalent when it came to the "risk-based approach": "While 42.5% agreed that the introduction of new compulsory requirements should only be limited to high-risk applications, another 30.6% doubt such limitation."[108] To give some colour on the range of views given in the response, we set out some extracts in **Table 3** below

Table 3: the Commission's AI White Paper – Examples of consultation feedback

#	Respondent	Feedback
1.	Ada Lovelace Institute	"The deployment of the concept of risk, let alone 'high risk', is problematic given the lack of a clear and accepted understanding of what the term means, particularly in the concept of autonomous systems."
2.	Facebook	"…there is a need for a clear distinction between the requirements that AI developers already need to comply with under the GDPR and those that go beyond GDPR."
3.	Huawei	"We would propose that a clear definition of "high risk" scenarios should be provided and reviewed regularly with transparent process and should be applied to all vendors."
4.	Microsoft	"…it is important to bear in mind that, in many cases, the use of AI – even in high-risk scenarios – may actually make products and services safer, better or more accurate than their non-AI counterparts."
5.	OpenAI	"AI is an omni-use technology where risks are not always immediately apparent, especially for systems with many use cases; the same system can be used in a low-risk sector, then quickly adapted to high-risk ones."

The October 2020 "non-paper". In some quarters the ambitious regulatory vision of the White Paper has been criticised as a premature move which threatens to stifle European innovation in a crucial sector which is already lagging behind its US and Chinese rivals. Von der Leyen's vision of swift AI regulation was dealt a blow in early October 2020 when a consortium of 14 EU Member States delivered a "non-paper" entitled *Innovation and Trustworthy AI: two sides of the same coin* to the Commission. The non-paper voiced a desire to "avoid setting burdensome barriers and requirements which can be a hindrance for innovation" and expressed other concerns about how "high risk" AI is defined.[109]

Whither Europe? While the significance of the "non-paper" was swiftly downplayed[110], it is likely to have created an additional headwind for the European AI regulatory process – at any rate, it is worth noting that

[108] European Commission, *Public Consultation on the AI White Paper: Final Report* (November 2020) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68462>.

[109] Various EU Member States, *Innovative and Trustworthy AI: two sides of the same coin – position paper on behalf of Denmark, Belgium, the Czech Republic, Finland, France, Estonia, Ireland, Latvia, Luxembourg, the Netherlands, Poland, Portugal, Spain and Sweden* (8 October 2020) <Non-paper - Innovative and trustworthy AI: two sides of the same coin | Publication | The Netherlands at International Organisations (permanentrepresentations.nl)>.

[110] See para entitled "Nothing to see here…" Janosch Delcker, *Politico AI: Decoded* (21 October 2020) <POLITICO AI:Decoded: Europe divided — The 'Access Now' files — Crunch time – POLITICO>.

AI rules have since been quietly dropped from the Commissions 2021 Work Programme[111], having been given top billing in 2020.[112] However, it is unlikely that the non-paper will completely derail the European drive towards overarching rules on AI; if it has a measurable effect it will be to delay and narrow its scope.

29. **The US: reluctant to burden US enterprise?** The US Government pipped the Commission to the post at the start of 2020 by publishing its own AI regulatory guidance in a draft Memo[113] in January, a month ahead of the Commission. In its sometimes strongly worded desire to "avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth", the Memo also signals reasonably clear philosophical differences with the European position. The Memo offers less in the way of regulatory detail than the Commission's AI White Paper (**E.28**), but there are some similarities. For instance, the Memo and the White Paper chime on the subject of conformity testing, with the Memo declaring that "targeted agency conformity assessment schemes… will be essential". It remains to be seen whether the Biden administration will depart from this *laissez faire* approach.

30. **The global tussle to set standards.** While some important foundations in AI regulation were set out in 2020, the bigger picture is still one of fractious geopolitics. This remains an important lens through which to see developments. For instance, the European White Paper highlights the Commission's expansive regulatory field of vision. Just as it did with GDPR, the Commission is clear that a European AI regulation should bite all over the world: "In the view of the Commission, it is paramount that the requirements are applicable to all relevant economic operators… whether they are in the EU or not." Perhaps for this reason, the White Paper was not particularly warmly received in Washington, with US Government officials remarking on its "clumsy attempts to bucket AI-powered technologies as either 'high risk' or 'not high risk'".[114]

31. ***The* Global *Partnership on Artificial Intelligence ("GPAI").*** In spite of these differences, an important development in 2020 was the founding of the GPAI, a multilateral group consisting of the G7 nations and several others[115], whose stated aim is to "support the responsible and human-centric development and use of AI in a manner consistent with human rights, fundamental freedoms and our shared democratic values."[116] The US initially refused to join the GPAI, reportedly over concerns that too much focus on regulation would hamper US AI innovation, but reversed the decision in May 2020.[117] A senior government representative explained the US's reasoning: "AI is being twisted by authoritarian regimes to violate rights… In this new forum, like-minded nations will work together to encourage the development of AI in line with our shared values.[118]

32. **The UK?**

No appetite for "cross-cutting" regulation... For several years now the UK Government has expressed a desire to avoid rushing to implement sweeping AI rules. In April 2018, for instance the UK House of Lords

---

[111] See here: <2021_commission_work_programme_annexes_en.pdf (europa.eu)>.
[112] See here: <resource.html (europa.eu)>.
[113] Available here: <2019-CATS-5830-REV_DOC--DraftOMBMemoonRegulationofAI101019.docx (whitehouse.gov)>.
[114] YouTube, *America's Global Tech Leadership: A Conversation with U.S. CTO Michael Kratsios* (20 February 2020) <America's Global Tech Leadership: A Conversation with U.S. CTO Michael Kratsios - YouTube>.
[115] At the time of writing: Australia, Brazil, Canada, France, Germany, India, Italy, Japan, Mexico, the Netherlands, New Zealand, Poland, the Republic of Korea, Singapore, Slovenia, Spain, the United Kingdom, the United States and the European Union.
[116] GPAI, *Joint statement from founding members of the Global Partnership on Artificial Intelligence* <Joint statement from founding members of the Global Partnership on Artificial Intelligence - GOV.UK (www.gov.uk)>.
[117] See Mia Hunt, Global Government Forum, *US abandons boycott of global AI partnership* (31 May 2020) <US abandons boycott of global AI partnership – Government & civil service news (globalgovernmentforum.com)>.
[118] Michael Kratsios, Wall Street Journal, *Artificial Intelligence Can Serve Democracy* (27 May 2020) <Artificial Intelligence Can Serve Democracy - WSJ>.

Select Committee report on AI (see **D.25**) found that "AI-specific regulation is not appropriate at this stage" and that "[e]xisting regulators are best placed to regulate AI in their respective sectors".[119] Almost three years later, in December 2020, the Select Committee on AI published an update in which its position was unchanged: "The challenges posed by the development and regulation of AI cannot currently be tackled by cross-cutting regulation… Sector-specific regulators are better placed to identify gaps in regulation, and to learn about AI and apply it to their sectors."[120] A UK Government contributor to the Select Committee's report summarised the UK Government's position:

> "The approach we have been taking across government is that the sectors are best placed to identify the regulation needed in their sphere… The regulator for the relevant sector has responsibility for determining what is needed in the sector and can draw on central resource from government to help understand that.[121]

… but important policy and institutional developments. Even though there has been less action on the regulatory front in the UK, AI is front and centre of the UK's industrial strategy. In its 2017 Industrial Strategy White Paper, the UK Government identified "AI and data" as one of four "Grand Challenges" (policy focal points).[122] In April 2018, the UK Government announced a significant investment program as part of its "AI Sector Deal".[123]

This policy focus led to the establishment of three key AI-focused bodies in 2018: the AI Council, the Office for AI and the Centre for Data Ethics and Innovation. Currently their roles and relationships are a work in progress (none of these bodies has a clearly defined statutory role yet, though there are plans to formalise them). But, in summary:

- *AI Council* – "The AI Council is a non-statutory expert committee of independent members set up to provide advice to government and high-level leadership of the AI ecosystem."[124]
- *Office for AI* – the Office for AI is an AI "delivery body" set up jointly under the UK Government's Department for Business, Energy and Industrial Strategy and Department for Digital, Culture, Media & Sport. Its roles include supporting the AI Council, overseeing the implementation of the AI Grand Challenge and creating and delivering the UK Government's AI strategy generally. In the first half of 2020, the Office for AI published guidance on the use of AI in the public sector and AI procurement (see **F.34**).
- *Centre for Data Ethics and Innovation* ("**CDEI**") – the CDEI's role is "to provide Government with access to independent, impartial and expert advice on the ethical and innovative deployment of data and artificial intelligence."[125] In its 2019/20 work programme, the CDEI has focused on reviews of online targeting and algorithmic bias.

Other significant bodies in the UK include the ICO (see para **D.21** above) whose role enforcing data protection legislation in the UK makes it important for AI, the Alan Turing Institute and the Open Data Institute.

---

[119] House of Lords Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?*, p. 7.
[120] House of Lords Select Committee on Artificial Intelligence, *AI in the UK: No Room for Complacency*, HL Paper 196 (December 2020) <AI in the UK: No Room for Complacency (parliament.uk)>, p. 17.
[121] *AI in the UK: No Room for Complacency*, pp. 13-14.
[122] HM Government, *Industrial Strategy: Building a Britain fit for the future* (November 2017) <Industrial Strategy: building a Britain fit for the future - GOV.UK (www.gov.uk)>, pp. 36-41.
[123] HM Government, *AI Sector Deal* (updated May 2019) <AI Sector Deal - GOV.UK (www.gov.uk)>.
[124] AI Council, *AI Council Terms of Reference* <AI Council Terms of Reference (publishing.service.gov.uk)>, p. 1.
[125] HM Government, *CDEI Framework Agreement* (20 March 2019) <Framework_Agreement_with_CDEI.pdf (publishing.service.gov.uk)>.

An interesting development came in September 2020 with the signing of a declaration between the US and the UK "on co-operation in Artificial Intelligence Research and Development."[126] The significance of this document, on AI regulation or otherwise, remains to be seen.

33. **Conclusion: the rising tide of regulation.** It is highly likely that rules and regulations specifically aimed at AI will emerge in the coming years, but 2020 itself was a mixed year for legislators hoping to draft them: there have been both significant steps forward (the Commission's White Paper (**E.28**) and the GPAI (**E.30**) and some setbacks (the 'non paper' (**E.28**)). For now, the guiding imperatives are economic and geopolitical. The rulebook will probably follow these lines.

F. AI IN THE ORGANISATION: ETHICS AND GOVERNANCE

34. **Introduction.** Since our last version of this white paper (September 2018), the number of reports, guidelines and codes of conduct from both government and AI industry stakeholders has continued to expand. Industry observer AlgorithmWatch has now identified over 160 documents of this type, the overwhelming majority of which come from Europe and the US.[127]

    In 2020 the UK Government's output focused more on practical aspects, like AI procurement, including:

    - NHS[X]'s *A Buyer's Guide to AI in Health and Care*, November 2020;[128]
    - the Office for AI's *Guidelines for AI Procurement*, June 2020;[129] and
    - the Government Digital Service and the Office for AI's *Guide to using AI in the Public Sector*, January 2020.[130]

    These publications are the latest in a growing corpus of UK Government AI ethics guidance.[131] There have also been some important multilateral developments, including:

    - the G20's *AI Principles*, June 2019;[132] and
    - the OECD's *Principles on Artificial Intelligence*, May 2019.[133]

35. **AI governance – general.** Beginning with Open Source Software governance 15 or so years ago, a structured approach to IT-related governance has become widely adopted 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 area of data protection

[126] Available here: <Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Artificial Intelligence Research and Development - GOV.UK (www.gov.uk)>.
[127] AlgorithmWatch, *AI Ethics Guidelines Global Inventory* <AI Ethics Guidelines Global Inventory (algorithmwatch.org)>. As at the date of the inventory's last update (April 2020), eight of these documents were classified as 'binding agreements', versus 44 'voluntary commitments' and 115 'recommendations'. See <About – AI Ethics Guidelines Global Inventory (algorithmwatch.org)> for more details.
[128] Available at: <A Buyer's Guide to AI in Health and Care - NHSX>.
[129] Available at: <Guidelines for AI procurement - GOV.UK (www.gov.uk)>.
[130] Available at: <A guide to using artificial intelligence in the public sector - GOV.UK (www.gov.uk)>.
[131] Helpfully summarised by UK Government's Department for Digital, Culture Media & Sport in its *Data ethics and AI guidance landscape* webpage in July 2020 (although an observer may conclude that the need for 'guidance' on the guidance points to a need to streamline and rationalise).
[132] Available at: <20190609 Ministerial Statement on Trade and Digital Economy (annex) (g20-insights.org)>.
[133] Available at: <OECD Principles on Artificial Intelligence - Organisation for Economic Co-operation and Development>.

in the run up to GDPR implementation, 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.[134]

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.36**) and the UK Government for AI and data ethics policy and processes (**F.37**).

Table 4: AI Principles – Microsoft (January 2018) and Google (June 2018)

#	Microsoft – AI Principles[135]	Google – AI Principles[136]
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**

36. **AI principles.** Both Microsoft and Google published in 2018 a set of principles to guide AI development, and these are set out at **Table 4** 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.

37. **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, with significant revisions made in September 2020) sets out key principles for appropriate use of data in the public sector. The

[134] See Kemp IT Law, *Legal Aspects of Cloud Computing: Cloud Security* (June 2018) <http://www.kempitlaw.com/wp-content/uploads/2018/06/Cloud-Security-White-Paper-KITL-v1.0-June-2018.pdf>, para C.19.

[135] Microsoft, *Responsible AI* <Responsible AI principles from Microsoft>. 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) <The-Future-Computed_2.8.18.pdf (microsoft.com)> , pp. 51–83.

[136] Google, *Artificial Intelligence at Google: Our Principles* <Our Principles – Google AI>. 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 violate internationally accepted norms; and (iv) that breach the principles of international law and human rights.

Framework is designed to be able to be overlaid onto data focussed public sector projects. There are two key parts to its structure:

- 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 the 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 5** below sets out the principles, specific actions and areas of additional guidance.

38. **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 and datasets they procure and use 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) was established in October 2017 and, at the time of writing, has published several preliminary technical reports including in July 2020 an overview of trustworthiness in AI.[137]

Sub-Committee 42 is currently working on 23[138] further standards and related documents, including technical reports on the robustness of neural networks[139] and AI use cases[140] as well as guidelines on data quality[141] and bias in AI systems.[142]

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 5: Summary of September 2020 UK Government Data Ethics Framework[143]

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")

[137] ISO/IEC TR 24028:2020.
[138] Listed at: <ISO - ISO/IEC JTC 1/SC 42 - Artificial intelligence>.
[139] ISO/IEC TR 24029-1.
[140] ISO/IEC CD TR 24030.
[141] ISO/IEC AWI 5259-2, ISO/IEC WD 5259-3 and ISO/IEC WD 5259-4.
[142] ISO/IEC DTR 24027.
[143] Government Digital Service, *Data Ethics Framework* (September 2020) <Data Ethics Framework - GOV.UK (www.gov.uk)>.

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 your project	**SA1.7** – Ensure there is a clear articulation of the 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

39. **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 make new statute law and the courts decide disputes and make new case law. AI is already another fascinating area for IT lawyers.

Chris Kemp
Kemp IT Law, London
February 2021
chris.kemp@kempitlaw.com
Tel: +44 (0)20 3011 1678

Annex: Glossary of terms used

Acronym	*Term*	*Where first used*
AEVA	The Automated and Electric Vehicles Act 2018	C.18
AI	Artificial Intelligence	A.1
AIaaS	AI as a Service	C.15
API	Application Programming Interface	C.15
AKI	Acute Kidney Injury	D.21
BMJ	British Medical Journal	A.2
BSI	British Standards Institution	C.18
CAV	Connected and Autonomous Vehicle	C.17
CCAV	Centre for Connected and Autonomous Vehicles	C.18
CDEI	Centre for Data Ethics and Innovation	E.32
CDPA	Copyright, Designs and Patents Act 1988	D.24
CLI	Command Line Interface	B.12
CPU	Central Processing Unit	B.10
DfT	UK Department for Transport	C.18
DPA 2018	Data Protection Act 2018	F.37
EDPB	European Data Protection Board	C.18
Epoch	Number of training data blocks	B.11, Figure 4
FCA	Financial Conduct Authority	C.16
GDPR	General Data Protection Regulation	D.21
GPAI	Global Partnership on AI	E.30
GPS	Global Positioning System	C.17
GPU	Graphics Processing Unit	A.4
GUI	Graphical User Interface	B.12
HARPS	Highly Automated Road Passenger Services	C.18
HLEG	High Level Expert Group on AI	E.28
IMU	Inertial Measurement Unit	C.18
ICO	Information Commissioner's Office	C.18
IPR	Intellectual Property Rights	D.25
ISO	International Organization for Standardization	A.3
LIDAR	**L**ight **D**etection **a**nd **R**anging	C.17
LSA	Legal Services Act 2007	C.16
LSB	Legal Services Board	C.16
LSP	Legal Service Provider	C.16
NCCID	National COVID-19 Chest Imaging Database	A.2
NLP	Natural Language Processing	A.4
PA	Patents Act 1977	D.24
PII	Professional Indemnity Insurance	C.16
PRA	Prudential Regulatory Authority	C.16
RADAR	**Ra**dio **D**etection **a**nd **R**anging	C.17
SCCF	SRA Code of Conduct for Solicitors, registered European lawyers and registered foreign lawyers	C.16
SCCS	SRA Code of Conduct for Firms	C.16
SRA	Solicitors Regulatory Authority	C.16
UK GDPR	The retained EU law version of the GDPR	D.21
UK IPO	UK Intellectual Property Office	D.24

KEMP IT LAW

IT Law at the Apex

Chris Kemp
Associate

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