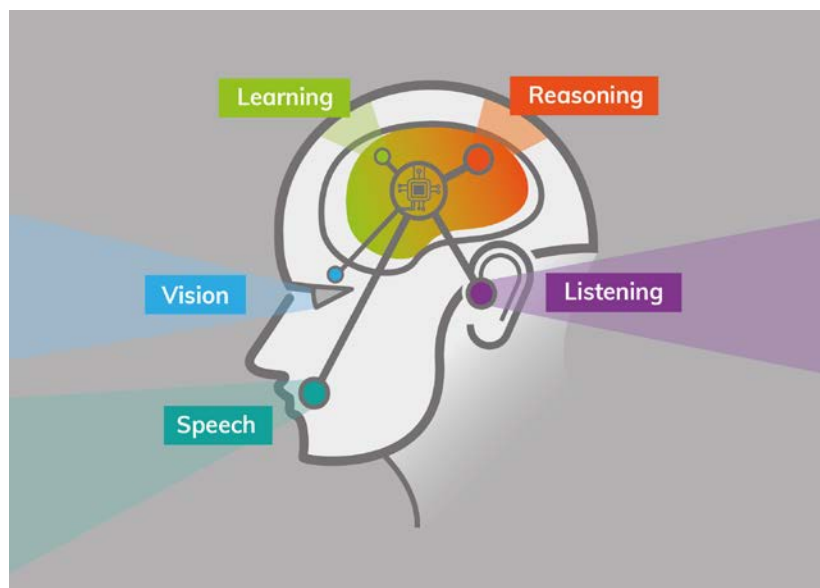




Legal Aspects of Artificial Intelligence (v2.0)

Richard Kemp
September 2018



This is a companion piece to our breakfast seminar to be held in London on Wednesday, 17 October 2018 – details and registration at <http://www.kempitlaw.com/managing-the-legal-aspects-of-artificial-intelligence/>

KEMP IT LAW

IT Law at the Apex



This is a companion piece to our breakfast seminar to be held in London on Wednesday, 17 October 2018 – details and registration at <http://www.kempitlaw.com/managing-the-legal-aspects-of-artificial-intelligence>

LEGAL ASPECTS OF AI (v2.0): TABLE OF CONTENTS

Para	Heading	Page	Para	Heading	Page
A.	INTRODUCTION	1	19.	Smart contracts: regulatory and legal aspects	18
1.	Artificial Intelligence in the mainstream	1	20.	Practical scenarios illustrating the regulatory and legal impact of AI	20
2.	What is 'Artificial Intelligence'?	1	D.	LEGAL ASPECTS OF AI.....	21
3.	The technical context.....	2	21.	Introduction.....	21
4.	The business context.....	2	22.	Some common misconceptions	21
5.	The legal, policy and regulatory context.....	2	23.	AI: policy and regulatory approaches.....	22
6.	Scope and aims of this white paper.....	3	24.	AI and data protection	23
B.	THE TECHNOLOGIES AND STREAMS OF AI 4		25.	AI and agency law	27
7.	The cloud and AI as twinned convergences: importance of the cloud	4	26.	AI and contract law.....	27
8.	AI: convergence, technologies and streams	4	27.	AI and intellectual property: software – works/ inventions generated/ implemented by computer	28
9.	Machine processing: Moore's law and GPUs....	5	28.	AI and intellectual property: rights in relation to data.....	29
10.	Machine learning: deep, supervised and unsupervised learning.....	6	29.	AI and tort law: product liability, negligence, nuisance and escape	31
11.	Machine perception: NLP, expert systems, vision and speech.....	7	E.	AI IN THE ORGANISATION: ETHICS AND GOVERNANCE.....	33
12.	Machine control: robotics and planning	8	30.	Introduction.....	33
C.	AI IN PRACTICE: CASE STUDIES	9	31.	AI Governance - General	33
13.	Introduction	9	32.	AI Principles.....	33
14.	AI in legal services: market developments	9	33.	AI Governance – the UK Government's Data Ethics Framework.....	34
15.	AI in legal services: regulatory and legal aspects	11	34.	AI technical standards.....	36
16.	Connected and autonomous vehicles ('CAVs'): technology and market aspects.....	13	F.	CONCLUSION	36
17.	CAVs: regulatory aspects	14	35.	Conclusion.....	36
18.	Smart contracts and blockchain	17			

FIGURES, TABLES AND ANNEXES

Figure 1: Twinned convergences: the Cloud and AI	4	Table 1: CAVs - Four Modes of Driving and Six Levels of Automation	15
Figure 2: The main AI Streams	5	Table 2: AI Principles: Microsoft (January 2018) and Google (June 2018)	34
Figure 3: Neurons and networks	6	Table 3: Summary of June 2018 UK Government Data Ethics Framework	34
Figure 4: Microsoft Cognitive Toolkit: increasing speech recognition accuracy by epochs of training set use	7	Annex 1 – Eight hypothetical scenarios illustrating the legal and regulatory impact of AI.....	37
Figure 5: CAVs vehicles' on board sensors.....	14	Annex 2 – Glossary of terms used	45
Figure 6: Towards a common legal framework for data	30		

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE (V2.0)¹

A. INTRODUCTION

1. **Artificial Intelligence in the mainstream.** Since the first version of this white paper in 2016, the range and impact of Artificial Intelligence (**AI**) has expanded at a dizzying pace as the area continues to capture an ever greater share of the business and popular imaginations. Along with the cloud, 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.²
2. **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.³ Six years later, at a conference at Dartmouth College, New Hampshire, USA to investigate how machines could simulate intelligence, Professor John McCarthy was credited with introducing the term 'artificial intelligence' as:

'the science and engineering of making intelligent machines, especially intelligent computer programs'.

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".⁴

Another organises the range of definitions into a 2 x 2 matrix of four approaches – thinking humanly, thinking rationally, acting humanly and acting rationally.⁵

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."⁶

Most 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."⁷

¹ The main changes in v2.0 are (i) expanding Section B (AI technologies and streams); updating and extending Section C (case studies); (iii) in Section D, adding a new data protection and expanding the IP paragraphs; and (iv) new Section E (ethics and governance). All websites referred to were accessed in September 2018.

² *'The Fourth Industrial Revolution'*, Klaus Schwab, World Economic Forum, 2016.

³ *'Computing Machinery and Intelligence'*, Alan Turing, *Mind*, October 1950

⁴ *'The Quest for Artificial Intelligence: A History of Ideas and Achievements'*, Prof Nils J Nilsson, CUP, 2010.

⁵ *'Artificial Intelligence, A Modern Approach'*, Stuart Russell and Peter Norvig, Prentice Hall, 3rd Ed 2010, p. 2

⁶ 2382:2015 is the ISO/IEC's core IT vocabulary standard - <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en:term:2123769>

⁷ *'The Future Computed: Artificial Intelligence and its role in society'*, Microsoft, January 2018, p.28 - <https://news.microsoft.com/uploads/2018/01/The-Future-Computed.pdf>



3. **The technical context.** For fifty years after the 1956 Dartmouth conference, AI progressed unevenly. The last decade however has seen rapid progress, driven by growth in data volumes, the rise of the cloud, the refinement of **GPUs** (graphics processing units) 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.8** 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').

4. **The business context.** Many businesses that have not previously used AI proactively in their operations will start to do so in the coming months. Research consultancy Gartner predicts that business value derived from AI will increase by 70% from 2017 to total \$1.2tn in 2018, reaching \$3.9tn by 2022. By 'business value derived from AI', Gartner means the areas of customer experience, cost reduction and new revenue. Gartner forecasts that up to 2020 growth will be at a faster rate and focus on customer experience (AI to improve customer interaction and increase customer growth and retention). Between 2018 and 2022, "niche solutions that address one need very well, sourced from thousands of narrowly focused, specialist AI suppliers" will make the running. Cost reduction (AI to increase process efficiency, improve decision making and automate tasks) and new revenue and growth opportunities from AI will then be the biggest drivers further out.⁸
5. **The legal, policy and regulatory context.** The start point of the legal analysis is the application to AI of developing legal norms around software and data. Here, 'it's only AI when you don't know 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 data is the input data (training, testing and operational datasets); that data as processed by the computer; and the output data (including data derived from the output).

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.

⁸ 'Gartner Says Global Artificial Intelligence Business Value to Reach \$1.2 Trillion in 2018', John-David Lovelock, Research Vice President, Gartner, April 25, 2018 - <https://www.gartner.com/newsroom/id/3872933>



These rapid developments are leading governments and policy makers around the world to grapple with what AI means for law, policy and regulation and the necessary technical and legal frameworks.⁹

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

- overviews at Section B the elements and technologies of AI;
- provides at Section C four 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.14** and **C.15**), connected and autonomous vehicles (**C.16** and **C.17**), smart contracts (**C.18** and **C.19**) and practical scenarios from the automotive, space, banking, logistics, construction, transportation, domestic and healthcare sectors (**C.20** and Annex 1);
- reviews at section D the legal aspects of AI from the standpoints of policy and regulatory approaches (**D.23**), data protection (**D.24**), agency law (**D.25**), contract law (**D.26**), intellectual property law (**D.27** and **D.28**) and tort law (**D.29**); and
- considers at Section E ethics and governance of AI in the organisation (**E.30** to **E.34**Error! Reference source not found.).

⁹ See for example the following recent developments: **China**: 12 Dec 2017: Ministry of Industry & Information Technology (**MIIT**), 'Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018-2020)' - <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/>.

European Union: 18 April 2018: Commission Report, 'the European Artificial Intelligence landscape' - <https://ec.europa.eu/digital-single-market/en/news/european-artificial-intelligence-landscape>; 25 April 2018: Commission Communication, 'Artificial Intelligence for Europe' - <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>; 25 April 2018: Commission Staff Working Document, 'Liability for emerging digital technologies' - <https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies>.

Japan: 30 May 2017, Japan Ministry of Economy, Trade and Industry (**METI**), 'Final Report on the New Industrial Structure Vision' - http://www.meti.go.jp/english/press/2017/0530_003.html.

UK:

- 15 October 2017: independent report by Prof Dame Wendy Hall and Jérôme Pesenti, 'Growing the artificial intelligence industry in the UK' - <https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk>;
- 27 November 2017: white paper 'Industrial Strategy – building a Britain fit for the future' - <https://www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future>
- 13 March 2018: House of Lords Select AI Select Committee, 'AI in the UK: ready, willing and able?' - <https://www.parliament.uk/business/committees/committees-a-z/lords-select/ai-committee/news-parliament-2017/ai-report-published/>;
- 26 April 2018: policy paper 'AI Sector Deal' - <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal#executive-summary>
- 13 June 2018 DCMS consultation on the Centre for Data Ethics and Innovation. Annex B lists key UK reports on AI since 2015 - <https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-consultation>
- 28 June 2018: 'Government response to House of Lords AI Select Committee's Report on AI in the UK: ready, willing and able?' <https://www.parliament.uk/business/committees/committees-a-z/lords-select/ai-committee/news-parliament-2017/government-response-to-report/>.

USA: 10 May, 2018, 'White House Summit on Artificial Intelligence for American Industry' - <https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf>.

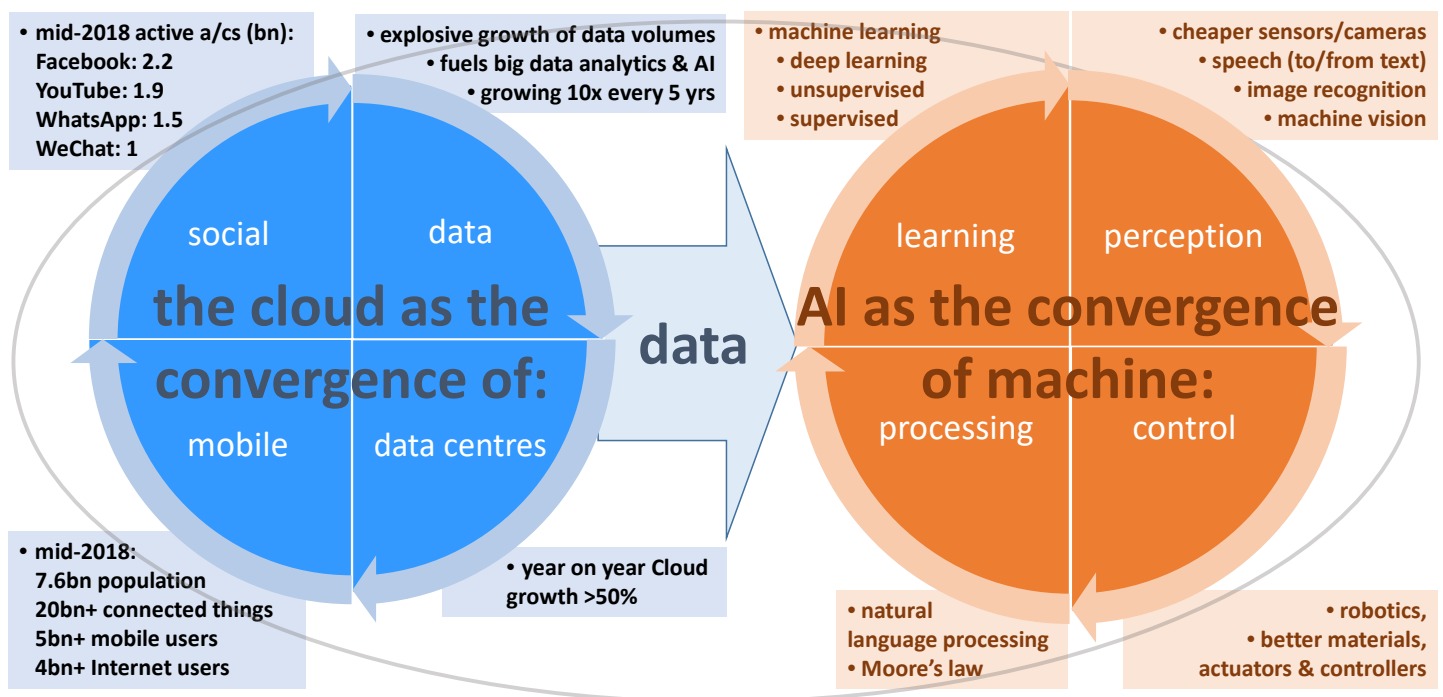


Annex 2 is a short glossary of terms used. This paper is general in nature and not legal advice. It is written as at 31 August 2018 and from the perspective of English law.

B. THE TECHNOLOGIES AND STREAMS OF AI

7. **The cloud and AI as twinned convergences: importance of the cloud.** Developments in AI have been fuelled by the ability to harness huge tides of digital data. These 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 are the engine rooms of the Cloud, where \$1bn+ investments in millions of square feet of space housing over a million servers accommodate current annual growth rates of between 50% and 100% of the three largest cloud service providers (**CSPs**), AWS (Amazon), Microsoft and Google. Internet, mobile and social media use at scale are in turn driving the cloud: for a global population of 7.6bn in mid-2018, there are currently estimated to be more than 20bn sensors connected to the internet, 5bn mobile users, 4bn internet users and 2.5bn social media users¹⁰. Increasing internet, mobile and social media use is in turn fuelling an explosion in digital data volumes, currently growing at an annual rate of around 40%, or ten times every five years. It is the availability of data at this scale that provides the raw material for AI.

Figure 1: Twinned convergences: the Cloud and AI



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

¹⁰ Statistics source: <https://www.computerworlduk.com/galleries/infrastructure/biggest-data-centres-in-world-3663287/> (data centres); <https://www.forbes.com/sites/johnkoetsier/2018/04/30/cloud-revenue-2020->

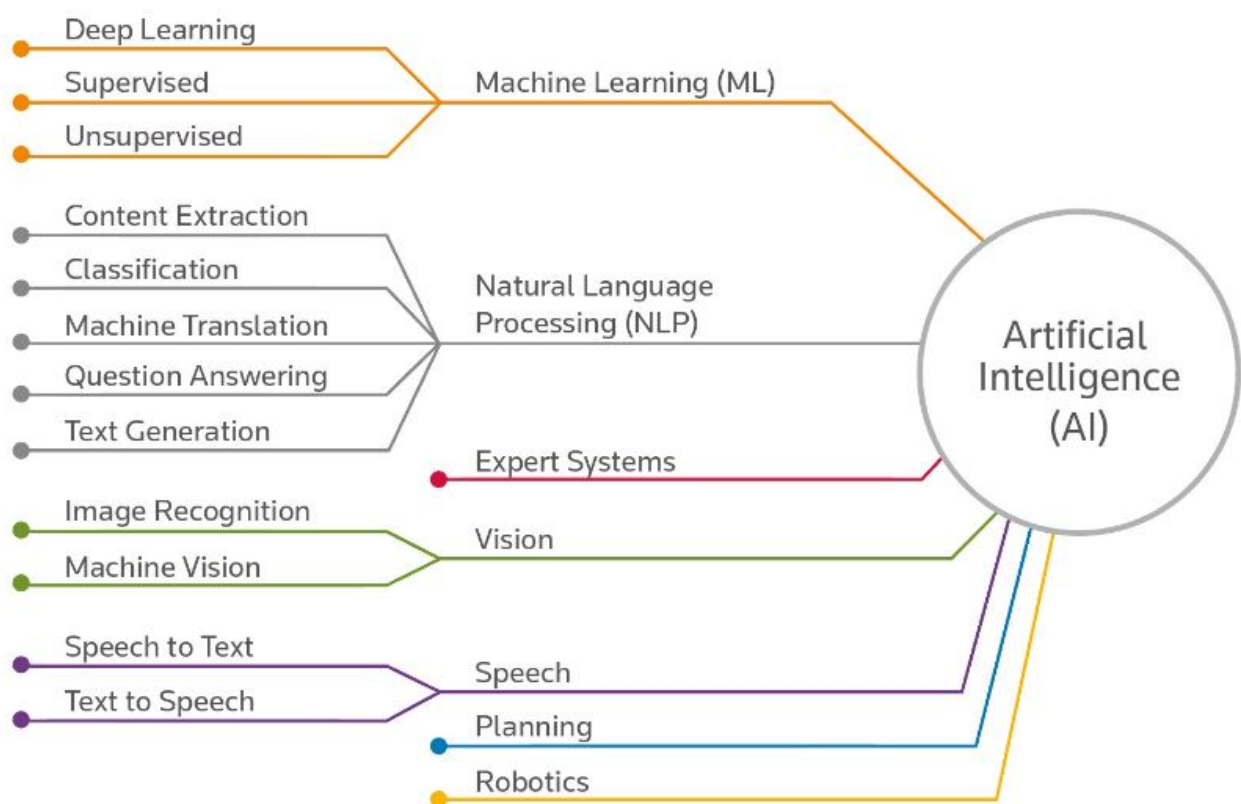


AI can be seen (see Figure 1 above) as the convergence of four areas of machine capability – processing (paragraph **B.9** below), learning (**B.10**), perception (**B.11**) and control (**B.12**). In the words of ‘*Humans Need Not Apply*’ by Jerry Kaplan, what has made AI possible is:

“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”.¹¹

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 streams¹²



9. **Machine processing: Moore’s law and GPUs.** In 1965 Intel co-founder Gordon Moore famously predicted that the density of transistors (microprocessors) on an integrated circuit (chip) would double approximately every two years. This rule held good for fifty years as computer processor

[amazons-aws-44b-microsoft-azures-19b-google-cloud-platform-17b/#f0d34727ee5a](#) (cloud growth rates); https://en.wikipedia.org/wiki/World_population (global population); <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/> (global internet connected sensors and things); <https://www.statista.com/statistics/617136/digital-population-worldwide/> (global internet, mobile and social media users).

¹¹ ‘*Humans Need Not Apply – A Guide to Wealth and Work in the Age of Artificial Intelligence*’, Jerry Kaplan, Yale University Press, 2015, pages 38 and 39.

¹² FullAI at <http://www.fullai.org/short-history-artificial-intelligence/> citing Thomson Reuters as source.



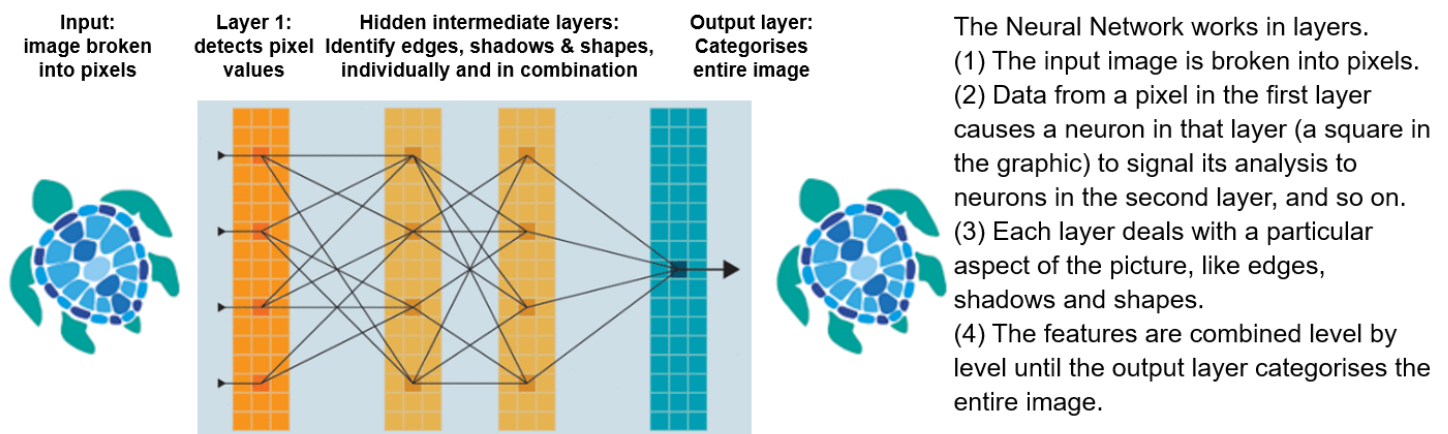
speeds reliably doubled every 18 to 24 months. Although Moore's Law is running out of steam as processor density increasingly produces counter-productive side-effects like excess heat, it remains a fundamental driver of the computer industry at the moment.

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.

10. **Machine learning: deep, supervised and unsupervised learning.** 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 by 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 neural networks as they seek to mimic the way the human brain works. For example, a computer may teach itself to recognise the image of a turtle by breaking the input data down into pixels then into layers, where information analysing the problem is passed from layer to layer of increasing abstraction and then combined in stages until the final output layer can categorise the entire image. How this process works is shown in Figure 3.

Figure 3: Neurons and networks¹³



Once trained, fine tuning the software decreases the error rate and increases the accuracy of predictions. To show how this happens, Microsoft provided in a 2016 blog¹⁴ an example of how the

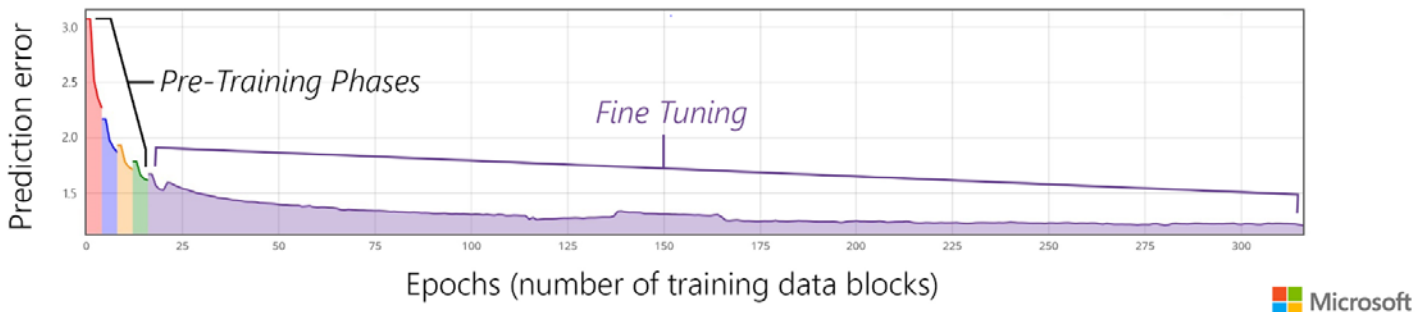
¹³ Sources: The Economist, Rise of the Machines, 9 May 2015, 'Layer Cake' graphic - <https://www.economist.com/briefing/2015/05/09/rise-of-the-machines>; House of Lords report – AI in the UK, Ready, Willing and Able, Figure 2, Deep Neural Networks, p.21

¹⁴ 'Microsoft releases beta of Microsoft Cognitive Toolkit for deep learning advances', 25 October 2016 <http://blogs.microsoft.com/next/2016/10/25/microsoft-releases-beta-microsoft-cognitive-toolkit-deep-learning-advances/#sm.0000lt0pxmj5dey2sue1f5pvp13wh>



Microsoft Cognitive Toolkit used training sets to increase training speech recognition accuracy. This is reproduced at Figure 4 below.

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



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 sectors¹⁵ including law (standardisable componentry of repeatable legal tasks), accountancy (auditing and tax), insurance (coupled with IoT sensors) and autonomous vehicles.

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

Labelling is time consuming, expensive and not easily transferable, 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. When Google DeepMind's AlphaGo program beat Lee Sedol, the eighteen times Go world champion, in March 2016 through a very unlikely move, AlphaGo initially used this type of unsupervised machine learning which it then reinforced by playing against itself (**reinforcement learning**).¹⁶

11. **Machine perception: NLP, expert systems, vision and speech.** Machine learning techniques when combined with increasingly powerful and inexpensive cameras and other sensors are accelerating machine perception – the ability of AI systems to recognise, analyse and respond to the data around them (whether as 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 **GUI** (graphical user interface) just as the GUI replaced the command line

¹⁵ See The Economist Special report: 'Artificial Intelligence – The Return of the Machinery Question', The Economist, 25 June 2016, page 42 <http://www.economist.com/news/special-report/21700761-after-many-false-starts-artificial-intelligence-has-taken-will-it-cause-mass>

¹⁶ See also 'Head full of brains, shoes full of feet – as AI becomes more human, it grows stronger' in The Economist, 1 September 2018, page 64 - <https://www.thesentientrobot.com/head-full-of-brains-shoes-full-of-feet-in-the-economist-1-september-2018/>



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. One third of all searches are predicted to be by voice by 2020. 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 Protection Advisor, launched in January 2018 and the first application to market in the Watson collaboration between IBM and Thomson Reuters, is a good example.¹⁷

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. Computers can now recognise objects in a photograph or video as accurately as people.¹⁸

Machine perception is also developing quickly in **speech**, where the error rate has declined to 5.1% - the same accuracy as a team of professional transcribers - as of August 2017¹⁹ and Amazon, Apple, Google and Microsoft invest heavily in their Alexa, Siri, Google Now and Cortana digital personal assistants.

12. **Machine control: robotics and planning.** Machine control is the design of robots and other automated machines using better, lighter materials and better control mechanisms to enhance the speed and sensitivity of machine response in 'sensing→planning→acting'. Machine control adds to the combination of machine learning and machine perception in a *static* environment the facility of interaction in, and manipulation of, a *mobile* 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. Annual global unit sales of industrial robots have risen by half from 250,000 in 2015 to 370,000 today and are forecast to rise to 510,000 in 2020. Global units of domestic consumer robots shipped have doubled from 4 to 8 million between 2015 and today, and are forecast to almost triple again to 23 million by 2025.²⁰

¹⁷ 'Thomson Reuters Introduces Data Privacy Advisor', 29 January 2018

<https://www.thomsonreuters.com/en/press-releases/2018/january/thomson-reuters-introduces-data-privacy-advisor.html>

¹⁸ See <https://blogs.microsoft.com/ai/microsoft-researchers-win-imagenet-computer-vision-challenge/>

¹⁹ 'Microsoft researchers achieve new conversational speech recognition milestone', 20 August 2017, <https://www.microsoft.com/en-us/research/blog/microsoft-researchers-achieve-new-conversational-speech-recognition-milestone/>

²⁰ Sources: industrial robots, Statista - <https://www.statista.com/statistics/272179/shipments-of-industrial-robots-by-world-region/>; domestic robots, Statista - <https://www.statista.com/statistics/730884/domestic-service-robots-shipments-worldwide/>



C. AI IN PRACTICE: CASE STUDIES

13. **Introduction.** Whilst AI can be broken down into its constituent technologies and streams irrespective of particular use cases, examining the practical application of AI to particular industry sectors will assist in providing a context for reviewing the legal aspects of an organisation's AI projects. Accordingly, this section works through four 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' (**C.14** and **C.15**);
- connected and autonomous vehicles as 'mobile AI' (**C.16** and **C.17**);
- smart contracts (**C.18** and **C.19**); and
- eight further practical scenarios (from the automotive, space, banking, logistics, construction, transportation, domestic and healthcare sectors) illustrating at high level for the main legal actors involved key regulatory and legal impacts of AI in the scenario (**C.20** and Annex 1).

Case Study 1 – AI in Legal Services

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

Background: AI and the legal services market. Legal services are a £30bn industry in the UK accounting for around 2% of GDP. They are representative of UK professional and business services generally, which together account for £190bn or 11% of UK GDP.

IT in legal services began in the 1970s with information retrieval, word processing and time recording and billing systems. The 1980s saw the arrival of the PC, office productivity software and the first expert systems; and the 1990s, email and 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 the 2010s around search and big data. The 2020s are predicted to be the decade of AI systems in the professions.²¹

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 93,000 in 2017. The rate of growth of UK in-house solicitors is even more dramatic, increasing by almost ten times from 2,000 in 1990 to 19,000 in 2017. The ratio of in-house to private practice solicitors in the UK now stands at 1:5, up from 1:20 in 1990.²²

These long term developments in IT use and lawyer demographics are combining with recent rapid progress in AI and increasing legal and regulatory complexity of business since the 2008 financial crisis 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

²¹ See further 'The Future of the Professions: How Technology Will Transform the Work of Human Experts', Richard and Daniel Susskind, Oxford University Press, 2015, page 160.

²² Sources: Law Society Annual Statistic Reports, 1997-2017. For a summary of the 2017 report, see <http://www.lawsociety.org.uk/support-services/research-trends/annual-statistics-report-2017/>



(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, RAVN and ROSS to innovate in these areas. 'Lawtech' corporate activity continues to be active, with document management developer iManage acquiring RAVN (May 2017), online legal solutions provider LegalZoom raising \$500m (July 2018) and Kira raising \$50m, Big 4 accounting firm EY acquiring legal automation firm Riverview and AI start-up Atrium raising \$65m in a financing led by US venture capital firm Andreessen Horowitz (all in September 2018).²³

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 ('AlaaS') 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 – 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 analysing higher value work;
- network effects will lead to consolidation as the preference develops to 'use the systems that everyone uses'.

How quickly will AI arrive? AI, like all major law firm IT systems is not easy to deploy effectively, and there are several hurdles to overcome, including, structuring and labelling training datasets correctly, deciding on the right number of training iterations to balance accuracy and risk, security and cultural inhibitions 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.²⁴ Another survey, of 200 in-house lawyers, found that the main hurdles to AI adoption in-house were cost, reliability and

²³ 'Andreessen Horowitz backs law firm for start-ups', Tim Bradshaw, Financial Times, 10 September 2018 - <https://www.ft.com/content/14b6767c-b4c1-11e8-bbc3-ccd7de085ffe>

²⁴ 'AI: The new wave of legal services', Legal Week, 20 September 2017 - <https://www.legalweek.com/sites/legalweek/2017/09/20/general-counsel-call-on-law-firms-to-share-the-benefits-of-new-artificial-intelligence-technology/?slreturn=20180814100506>



appetite for change:²⁵ 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 might take even longer.

15. 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**)²⁶ 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 list²⁷ so that most 'legal activities'²⁸ are unregulated.²⁹ 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.³⁰

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 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.

The SRA Handbook. The regulatory standards and requirements that the SRA "expects [its] regulated community to achieve and observe, for the benefit of the clients they serve and in the public interest" are contained in the SRA Handbook.³¹ At present, there are no regulatory

²⁵ 'Legal Department 2025, Ready or Not: Artificial Intelligence and Corporate Legal Departments', Thomson Reuters, October 2017 - https://static.legalsolutions.thomsonreuters.com/static/pdf/S045344_final.pdf

²⁶ <http://www.legislation.gov.uk/ukpga/2007/29/part/3>

²⁷ 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.

²⁸ 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.

²⁹ Contrast the position in the USA for example, where the US State Bar Associations much more zealously protect against the unauthorised practice of law.

³⁰ 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; (iii) 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; (iv) the Costs Lawyer Standards Board; (v) the Master of the Faculties (notaries); and (vi) 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.

³¹ <https://www.sra.org.uk/handbook/>



requirements specifically applicable to AI and the relevant parts of the SRA Handbook are the same ten overarching Principles³² and parts of the Code of Conduct³³ that apply to IT systems and services generally.

The Principles include acting in the best interests of the client, providing a proper standard of service, complying with regulatory obligations and running “the business effectively and in accordance with proper governance and financial risk management principles”.

The Code of Conduct is in 15 chapters and sits beneath the Principles setting out outcomes (mandatory) and indicative behaviours (for guidance). In addition to client care, confidentiality and relationship with the SRA, the relevant outcomes for IT services are mainly at Chapter 7 (business management) and include (i) clear and effective governance and reporting (**O(7.1)**), (ii) identifying, monitoring and managing risks to compliance with the Principles (**O(7.3)**), (iii) maintaining systems and controls for monitoring financial stability (**O(7.4)**), (iv) compliance with data protection and other laws (**O(7.5)**), (v) appropriate training (**O(7.6)**) and (vi) appropriate professional indemnity insurance (**PII**) cover (**O(7.13)**).

SRA Code of Conduct: outsourcing – O(7.10). Specific outcomes are also mandated at **O(7.10)** for outsourcing, which is described in the introduction to Chapter 7 as “using a third party to provide services that you could provide”. The use of a third party AI platform (but not a platform proprietary to the firm) in substitution for work carried out by staff at the firm is therefore likely to be ‘outsourcing’ for this purpose. Under O(7.10), a firm must ensure that the outsourcing (i) does not adversely affect compliance, (ii) does not alter its obligations to clients and (iii) is subject to contractual arrangements enabling the SRA or its agent to “obtain information from, inspect the records ... of, or enter the premises of, the third party” provider. This information requirement is likely to be reasonably straightforward to comply with in the case of a third party AI platform used in-house but can give rise to interpretation difficulties for cloud and other off-premises services.

Client engagement terms: LSPs. LSPs using AI in client service delivery should consider including 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 minimum³⁴ 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

³² <https://www.sra.org.uk/solicitors/handbook/handbookprinciples/content.page> The Principles have been in effect since October 2011 and were made by the SRA Board under (i) ss. 31, 79 and 80 of the Solicitors Act 1974, (ii) ss. 9 and 9A of the Administration of Justice Act 1985 and (iii) section 83 of the Legal Services Act 2007 with the approval of the Legal Services Board under the Legal Services Act 2007, Sched 4, para 19. 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.

³³ <https://www.sra.org.uk/solicitors/handbook/code/content.page>

³⁴ LSPs must hold an “appropriate level” of PII (**O(7.13)**) which under the Insurance Indemnity Rules 2012 must be not less than £3m for Alternative Business Structures, limited liability partnerships and limited companies and £2m in all other cases.



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)

16. Connected and autonomous vehicles ('CAVs'): market and technology aspects.

The CAV market: Statistics provider Statista estimates the global stock of passenger cars and commercial vehicles in use in 2018 at 1.4bn, of which roughly 100m will be sold in 2018. Of the total stock, Statista estimates that 150m are connected today and predicts that this will rise to a quarter (360m) by 2022. Connected vehicle revenue (connected hardware and vehicle services and infotainment services) is estimated at \$34bn today (up from \$28bn in 2016) and predicted to rise to almost \$50bn by 2022, a compound growth rate of 10% over the next four years.³⁵ 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.

'Vehicles', 'connectedness' and 'autonomy'.³⁶ By **'vehicles'** we mean passenger cars and commercial vehicles, although AI of course will impact 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. **'Autonomous'** means that the vehicle itself is 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 coordinated 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 (**radio detection and ranging**), lidar (**light detection and ranging** – essentially laser-based radar to build 3D maps), sonar (**sound navigation and ranging**), cameras and ultrasound.

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

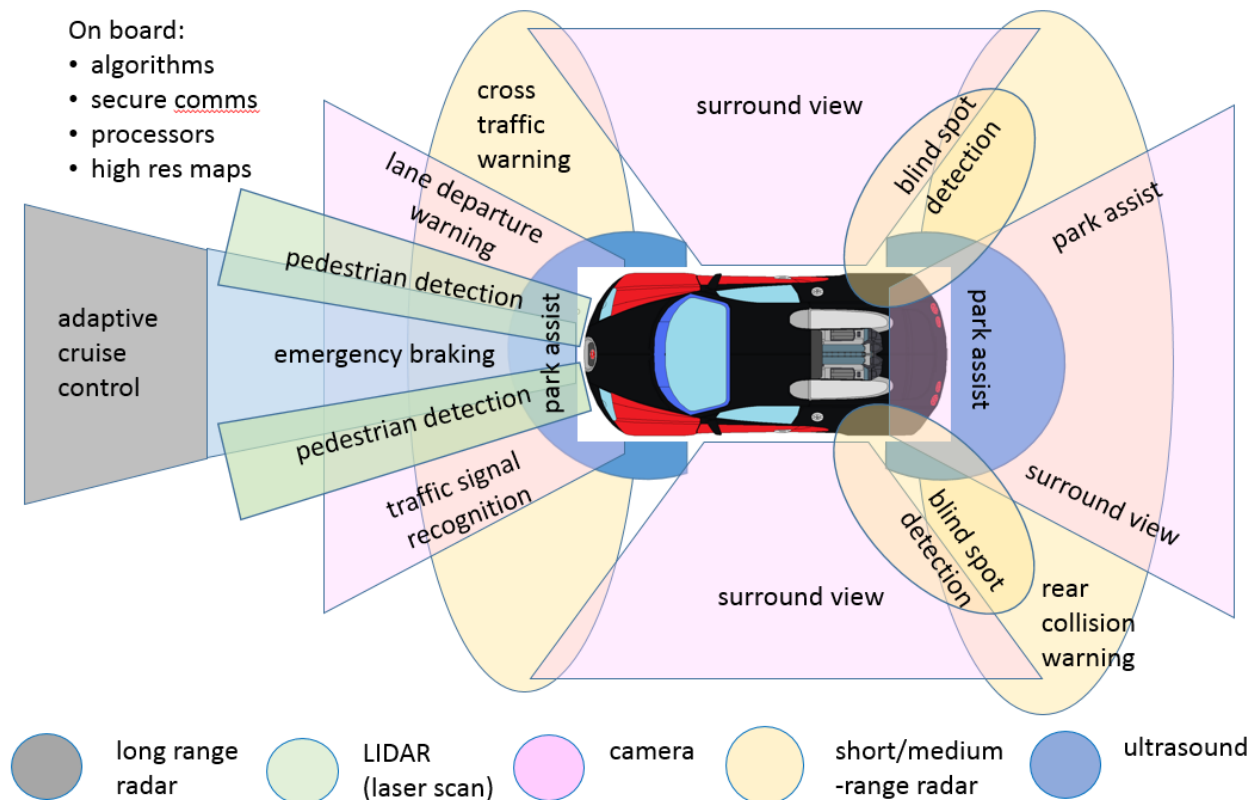
³⁵ Connected Car - <https://www.statista.com/outlook/320/100/connected-car/worldwide>

³⁶ For an excellent guide, see 'Technological Opacity, Predictability, and Self-Driving Cars', Harry Surden (University of Colorado Law School) and Mary-Anne Williams (University of Technology, Sydney), March 2016 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747491



with detailed driving feature information like traffic lights, signs and lane markings. These digital maps are increasingly updated dynamically in real time.

Figure 5 – CAVs' on board sensors³⁷



Sense → plan → act. The computer 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 representation to the digital map; and in the **acting** phase, the computer moves the vehicle accordingly by activating its driving systems.

17. CAVs: regulatory aspects.

Towards CAV regulation: issues to be addressed. Since the first of the UK Locomotive ('Red Flag') 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 autonomous vehicles predicates 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 autonomous vehicles 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;

³⁷ Source: adapted from OECD International Transport Forum paper, 'Autonomous and Automated Driving – Regulation under uncertainty', page 11, <http://www.itf-oecd.org/automated-and-autonomous-driving>



(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 has mapped³⁸ 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. It has set up the Centre for Connected and Autonomous Vehicles (**CCAV**) and, under the general approach '*Pathway to Driverless Cars*', published a detailed review of regulation for automated vehicle technologies³⁹ (February 2015) and a Code of Practice for testing⁴⁰ (July 2015) and carried out a wide ranging consultation on proposals to support advanced driver assistance systems (**ADAS**) and automated vehicle technology ('**AVT**')⁴¹ (July 2016 to January 2017). In March 2018, the CCAV commissioned the Law Commission, the statutory independent reviewer of English law to carry out a detailed, three year review "of driving laws to ensure the UK remains one of the best places in the world to develop, test and drive self-driving vehicles".⁴²

³⁸ SAE International Standard J3016 201401, '*Taxonomy and Definition of Terms Related to on-Road Motor Vehicle Automated Driving Systems*', 16 January 2014, http://standards.sae.org/j3016_201401/

³⁹ <https://www.gov.uk/government/publications/driverless-cars-in-the-uk-a-regulatory-review>

⁴⁰ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/446316/pathway-driverless-cars.pdf

⁴¹ '*Pathway to driverless cars consultation*', DfT/CCAV -

<https://www.gov.uk/government/consultations/advanced-driver-assistance-systems-and-automated-vehicle-technologies-supporting-their-use-in-the-uk>

⁴² '*Government to review driving laws in preparation for self-driving vehicles*', DfT, 6 March 2018 -

<https://www.gov.uk/government/news/government-to-review-driving-laws-in-preparation-for-self-driving->



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 AVT development. The UK has therefore decided to take a step by step approach, (i) confirming that AVT testing is permitted in the UK (February 2015), (ii) setting out applicable standards in the testing Code of Practice (July 2015), (iii) amending the Highway Code, for example to permit remote control parking (June 2018)⁴³ and (iv) addressing insurance for domestic CAV insurance (July 2018)⁴⁴. The DfT is also working on vehicle construction regulation and international standards for AVT.

CAVs and data protection. The data protection analysis of CAVs presents a number of complex questions. CAVs include a broad range of onboard devices that originate data. These devices include GPSs, 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 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 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".⁴⁵

In addition to general data protection questions, CAV use of personal data is likely to raise further issues around (i) device use as surveillance cameras/systems,⁴⁶ (ii) automated number plate recognition (ANPR) and other Automated Recognition Technologies (ART), (iii) audio recordings,⁴⁷ (iii) data sharing (with cloud service providers, insurance carriers and other CAV ecosystem participants) and (iv) AI/business intelligence further processing.⁴⁸ An explicitly governed approach to use of personal and other data in the CAV context, consisting of statements of principles, strategy, policy and processes and including tools like data protection impact assessments and privacy by design, is therefore likely to become indispensable.

[vehicles](#)

⁴³ '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', DfT news story, 17 May 2018 - <https://www.gov.uk/government/news/new-laws-pave-way-for-remote-control-parking-in-the-uk> following conclusion of the DfT's consultation on the UK Highway Code (19 December 2017 – 16 May 2018) - <https://www.gov.uk/government/consultations/remote-control-parking-and-motorway-assist-proposals-for-amending-regulations-and-the-highway-code>

⁴⁴ 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 - <http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted>

⁴⁵ 'Response to the CCAV's consultation "Pathway to Driverless Cars"', ICO, 9 September 2016 <https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1624999/df-pathway-to-driverless-cars-ico-response-20160909.pdf>

⁴⁶ See also 'In the picture: a data protection code of practice for surveillance cameras and personal information', ICO, September 2017 - <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

⁴⁷ See also *Southampton City Council v Information Commissioner*, February 2013 - <https://www.southampton.gov.uk/modernGov/documents/s18170/Appendix%204.pdf>

⁴⁸ See also 'Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)', Article 29 Working Party Opinion 03/2017, October 2017 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171



CAVs and cyber security. Cyber security has also emerged as a critical area of CAV and AVT 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).⁴⁹

Case Study 3 – Smart Contracts

18. Smart contracts and blockchain.

Blockchain/DLT terminology. Blockchain (or distributed ledger technology, **DLT**) is a comprehensive, always up to date database (**ledger**) combining cryptography and database distribution to “allow strangers to make fiddle-proof records of who owns what”.⁵⁰ Cryptography authenticates parties’ identities and creates immutable hashes (**digests**) of each ledger record, the current page of records (**block**) and the binding that links (**chains**) each block to the earlier ones in the database. The whole blockchain database is distributed to network participants (**miners**) who keep it up to date.

DLT platform characteristics. In traditional data storage, a single entity controls contributions to the database as holder of ‘a single version of the truth’. In DLT, participating entities hold a copy of the database and can contribute to it. **Governance** and **consensus** mechanisms ensure database accuracy and the ‘common version of the truth’ wherever the ledger is held. If anyone can contribute, the mode of the platform is **permissionless** and (usually) **public**. If the mode is **permissioned** the DLT platform is **private** and contributions are limited. Where consensus is achieved by way of mining, a **crypto-asset** (cryptocurrency) or **token** is required for value exchange.

DLT examples. DLT:

“over the past 2-3 years has emerged as a viable technology for addressing multi-party business processes and value exchange without complex shared data schemes and third-party intermediaries.”⁵¹

Ethereum is an example of a generic, public, permissionless DLT platform. Interbank Information Network, a DLT powered by Quorum, a permissioned variant of Ethereum, was set up by J.P. Morgan with Royal Bank of Canada and Australia and New Zealand Banking Group to trial DLT in banking applications and now has over 75 members. Hyperledger Fabric is a private, permissioned, modular, open source DLT framework (hosted by the Linux Foundation) for the development of DLT applications. Corda is also a private, permissioned open source DLT platform and was developed by R3 (an enterprise distributed database software firm that has developed since 2015 from its roots as a consortium of leading global financial services businesses) specifically for security and privacy

⁴⁹ ‘Key principles of vehicle cyber security for connected and automated vehicles’, DfT, 6 August 2017 - <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles>

⁵⁰ The Economist, 5–11 November 2016, page 10.

⁵¹ ‘5 ways blockchain is transforming Financial Services’, Microsoft, March 2018 - <https://azurecomcdn.azureedge.net/mediahandler/files/resourcefiles/five-ways-blockchain-is-transforming-financial-services/five-ways-blockchain-is-transforming-financial-services.pdf>



compliant enterprise applications. Ethereum operates Ether as its currency. Hyperledger Fabric and Corda do not operate currencies.⁵²

DLT, smart contracts and AI. “Smart contracts” are self-executing arrangements that the computer can make, verify, execute and enforce automatically under event-driven conditions set in advance. In DLT, they were initially the software tool that the database used to govern consensus about changes to the underlying ledger and used in this way are part of the operation of the DLT platform. However, potential use cases go much further, and the software can also be used in the application this sits on top of the DLT platform to make and execute chains or bundles of contracts linked to each other, all operating autonomously and automatically. Smart contracts have the potential to reduce error rates (through greater automation and lower manual involvement) and costs (removing the need for intermediation) and promise benefits from rapid data exchange and asset tracking, particularly for high volume, lower value transactions. Although not predicated on use of AI, DLT-based smart contracts when combined with machine learning and cloud-based, as a service processing open up new operating models and businesses.

Smart contract use cases. Smart contracts represent evolution not revolution. E- and m- commerce today already makes binding contracts for media, travel and other goods and services through data entry and exchange over the internet; and automatic algorithmic trading in financial markets pre-programmes AI systems to make binding trades and transactions when certain conditions are satisfied. Smart contracts take this to the next level by further reducing individual human intervention and increasing codification and machine use. Areas of potential development include contract management (legal), clearing and settlement of securities trades (financial services), underwriting and claims processing (insurance), managing electronic patient records (healthcare), royalty distribution (music and media) and supply chain management (manufacturing).

19. **Smart contracts: legal and regulatory aspects.** The world of smart contracts can be seen from a number perspectives. First, blockchain/DLT regulation; second, at the developer level, the DLT smart contract code will need to represent contract law norms; third, the smart contract platform operator will need to contract upstream with the developer and downstream with users; and fourth, each user will need to contract with the platform operator.

Regulation of crypto-assets, blockchain/DLT and smart contracts: in terms of regulation, a distinction arises between crypto-assets (digital- or crypto- currencies) on the one hand and blockchain/DLT and smart contracts on the other. The perception of crypto-assets has tended to become a little tainted over time. The UK House of Commons Treasury Committee in its September 2018 report noted that crypto-assets were especially risky because of their volatility and lack of security, inherent value and deposit insurance.⁵³ Further:

“[o]wing to their anonymity and absence of regulation, crypto-assets can facilitate the sale and purchase of illicit goods and services and can be used to launder the proceeds of serious crime

⁵² Ethereum: <https://www.ethereum.org/>. Interbank Information Network: <https://www.ft.com/content/41bb140e-bc53-11e8-94b2-17176fbf93f5> Hyperledger Fabric: <https://www.hyperledger.org/projects/fabric>. Corda: <https://www.corda.net/>.

⁵³ ‘Crypto-assets’, House of Commons Treasury Committee Report, 12 September 2018 - <https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf>



and terrorism. The absence of regulation of crypto-asset exchanges—through which individuals convert crypto-assets into conventional currency—is particularly problematic.” (page 43)

Accordingly, regulation of crypto-assets in the UK is very much on the cards:

“[g]iven the scale and variety of consumer detriment, the potential role of crypto-assets in money laundering and the inadequacy of self-regulation, the Committee strongly believes that regulation should be introduced. At a minimum, regulation should address consumer protection and anti-money laundering.” (page 44)

Aside from crypto-assets, blockchain/DLT and smart contracts however are essentially like other software systems. Whether they will be treated for regulatory purposes as critical system outsourcing (for example in the legal or financial services sector) will depend, as for other software systems, on how they are used and what they do, rather than on their intrinsic nature as blockchain/DLT or smart contracts. In addition, smart contracts (as software systems to make, verify, execute and enforce agreements under pre-agreed, event driven conditions) will be subject to general contract law norms and, when operating in sectors that are specifically regulated or subject to general regulation (for example, data protection or consumer protection) will be subject to those specific or general regulatory requirements.

Developer level: Smart contracts in code. In building the smart contract software, the developer will be representing as computer programs a system of normative, contractual rules – a sort of executable ‘Chitty on Contracts in code’. The database schema of the system’s information architecture – its formal structure and organisation - starts with the flow of information and instructions in the ‘real world’, takes it through levels of increasing abstraction and then maps it to a data model - the representation of that data and its flow categorised as entities, attributes and interrelationships - in a way that any system conforming to the architecture concerned can recognise and process. Software, as a set of instructions, is not unadjacent to a contract as both set binding rules determining outputs from inputs (‘if this, then that’).

The information architecture and data modelling of the smart contract system will therefore address, in software code, the whole world of contract possibilities that may arise in system use. These include contract formation; payment, performance and lifecycle issues; discharge, liability and resolution; conditionality, dependencies and relief events; audit trail and records generation and retention. The system will also need to cater for relevant regulatory aspects relating to the subject matter of the contracts it is executing – around personal data for example and any consumer and authorisation and compliance regulatory aspects.

Smart contract platform operator level:

- **Platform operator/developer contract.** At this level, the agreement between the smart contract developer and platform operator is a software ‘design, build and operate’ agreement – with elements of development, software licensing (if the developer is to retain IP) or transfer (if the IP is to be assigned to the platform operator) and/or service provision that IT lawyers will be familiar with. Particular care will need to be taken in mapping the ‘virtual world’ of the smart contracts to the real world contractual ecosystem at whose centre sits platform operator. In particular, risk allocation - the ‘what if’s’ of system errors, outages and failures – will need to be managed both contractually (through the governance, service level agreement, liability, indemnity and termination mechanisms) and as appropriate through insurance.



- **Platform operator/user contract.** The platform operator will need to put in place contract or use terms with each user of the platform. Here, the analogy is with stock exchanges and other trading venues which have detailed membership agreements, contractually binding operational rules, and a range of related agreements and policies regarding software, data licensing and system use and other relevant matters. The platform operator will need to ensure adequate governance and dispute resolution procedures to address the consequences for affected users and counterparties of any failure of the smart contract software anywhere in the ecosystem to operate in the way intended.

User level. The user joining any smart contract system will be presented with a series of standard form contracts that may be difficult in practice to change. Key issues for the user include:

- clarity about the extent of contracting authority that the user is conferring on the platform operator's smart contract system – for example, how does it address in all cases where the user is involved the basic issues of contract formation for contracts directly made with the user and any connected agreements on which its own agreements depend;
- evidential requirements (including auditing, record generation/retention and access to/return of data) for commitments entered into by the smart contract platform in the user's name;
- regulatory issues – control/processing of personal data; system security; regulatory authorisation and compliance requirements - for all/any other platform users, etc; and
- the normal range of contract lifecycle issues, including performance/availability, liability and risk; conditionality/dependencies; and supplier dependence and exit management.

Case Study 4 – Practical Scenarios from Different Industry Sectors

20. **Practical scenarios illustrating the regulatory and legal impact of AI.** In Annex 1 (pages 37 to 44 below) we have set out eight practical scenarios illustrating at high level the main legal and regulatory issues arising for the main legal actors in particular AI use cases from a number of industry sectors. The scenarios are:
- a) **automotive:** a car, ambulance and bus, all operating autonomously, collide at a road intersection;
 - b) **space:** multiple AI-enabled satellites coordinate with each another in space;
 - c) **banking:** separate smart contract systems incorrectly record a negotiated a loan agreement between lender and borrower;
 - d) **logistics:** companies use their AIs in their logistics, supply and manufacturing chains;
 - e) **construction:** construction firms use multiple autonomous machines to build an office block;
 - f) **transportation:** AI is used for the supply of transportation and services in smart cities;
 - g) **domestic:** multiple robots work with each other in the home; and
 - h) **healthcare:** medical and healthcare diagnostics and procedures are planned and carried out by and using AI and robotics.



D. LEGAL ASPECTS OF AI

21. **Introduction.** This section overviews relevant legal and regulatory 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 (paragraph **D.22**). Regulatory aspects of AI that are set to develop are then outlined (**D.23**). AI is then briefly considered in relation to the law of data protection (**D.24**) agency (**D.25**), contract (**D.26**), intellectual property rights for software (**D.27**) and data (**D.28**), and tort (**D.29**).

22. **Some common misconceptions.** Three misconceptions based on the fallacy that the embodiment of AI has the qualities of a legal person⁵⁴ 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 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.⁵⁵ 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.

⁵⁴ 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".

⁵⁵ On 16 February 2017 the European Parliament adopted a resolution making recommendations to the Commission on civil law rules on robotics - <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>. At paragraph 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 - http://europa.eu/rapid/press-release_IP-18-3362_en.htm.



23. **AI: policy and regulatory approaches.** As mentioned in the introduction at paragraph **A.5**, AI is giving governments and policy makers much to grapple with. High level questions arise: what interests should AI regulation protect? Should existing regulatory structures be adapted or new ones created? How should regulatory burdens be kept proportionate? What role should central government play? An October 2016 report from the US Obama administration '*Preparing for the Future of Artificial Intelligence*' set out risk based public protection and economic fairness as the key regulatory interests, using current regulation as the start point where possible:

"AI has applications in many products, such as cars and aircraft, which are subject to regulation designed to protect the public from harm and ensure fairness in economic competition. How will the incorporation of AI into these products affect the relevant regulatory approaches? In general, the approach to regulation of AI-enabled products to protect public safety should be informed by assessment of the aspects of risk that the addition of AI may reduce alongside the aspects of risk that it may increase. If a risk falls within the bounds of an existing regulatory regime, moreover, the policy discussion should start by considering whether the existing regulations already adequately address the risk, or whether they need to be adapted to the addition of AI. Also, where regulatory responses to the addition of AI threaten to increase the cost of compliance, or slow the development or adoption of beneficial innovations, policymakers should consider how those safety or market fairness."⁵⁶

The example of legal services AI at paragraph **C.15** above shows how AI can fit within a current regulatory structure without much change. Here, bought in AI will count as outsourcing under Outcome 7.10 of the SRA Code of Conduct in the UK's regime of regulated legal services.

The approach of the UK to CAVs outlined at **C.17** shows how existing regulatory structures can successfully be adapted to protect the public and ensure fairness. Here, regulatory change is consulted widely in advance and then broken down into bite sized chunks - facilitating testing, amending the Highway Code, addressing CAV insurance and addressing vehicle construction.

An important policy question for government is whether to centralise its AI expertise or to decentralise it across government departments. The US '*Future of AI*' report appeared to advocate common goals for the US federal government and agencies rather than centralisation. In the UK, HM Government in its November 2017 Industrial Strategy white paper identified "putting the UK at the forefront of the AI and data revolution" as one of four "Grand Challenges". The white paper was followed up in April 2018 with an '*AI Sector Deal*' policy paper published by the Departments for Business, Energy and Industrial Strategy (**DBEIS**) and Digital, Culture, Media & Sport (**DDCMS**) and building on the recommendations of the October 2017 Hall-Pesenti report. These papers, together with the March 2018 House of Lords '*AI in the UK: ready willing and able?*' report and the June 2018 Government response to that report, propose a new UK government framework for AI consisting of:

- a new AI Council "to bring together respected leaders in the field from academia and industry";
- a new Office for Artificial Intelligence as the "new delivery body within the government";

⁵⁶ '*Preparing for the Future of Artificial Intelligence*', Executive Office of the President and the National Science and Technology Council, Committee of Technology, 12 October 2016, page 11
https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf



- a new Centre for Data Ethics and Innovation (which the DDCMS consulted on in June – September 2018); and
- the Alan Turing Institute, as the national institute for data science and AI.⁵⁷

The regulatory position in the UK for AI is further complicated as we cross the thresholds of Brexit and the fourth industrial revolution at the same time. Brexit will continue to take up a significant part of the civil service workload. This will inevitably make it more difficult at this seminal time for AI policy makers to take effective and high quality decisions. The UK IT industry will need to shout loud on AI issues to make its voice heard above the Brexit din.

24. AI and data protection.

General applicability of the GDPR to AI.⁵⁸ The GDPR, which came into effect on 25 May 2018, applies to personal data used in AI. In her foreword to the ICO's March 2017 paper, '*Big data, artificial intelligence, machine learning and data protection*', the Commissioner said (at page 3):

"it's clear that the use of big data has implications for privacy, data protection and the associated rights of individuals – rights that will be strengthened when the GDPR is implemented. Under the GDPR, stricter rules will apply to the collection and use of personal data. In addition to being transparent, organisations will need to be more accountable for what they do with personal data. This is no different for big data, AI and machine learning."⁵⁹

In addition to the basic principles of GDPR compliance at Arts. 5 and 6 (lawfulness through consent, contract performance, legitimate interests, etc.; fairness and transparency; purpose limitation; data minimization, accuracy; storage limitation; and integrity and confidentiality), AI raises a number of further issues. These include the AI provider's role as data processor or data controller, anonymization and other AI data protection compliance tools, research and pseudonymization, and profiling/automated decision-making. These are now briefly considered.

AI provider as data processor or controller? By Art. 4(7) a person who determines "the purposes and means" of processing personal data is a data controller and under the 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 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 GDPR compliant structuring of the relationship and to allocating risk and responsibility.

However, the borderline between controller and processor can be fuzzy in practice.⁶⁰ Where it lies in the AI context was considered for the first time in the UK in the ICO's July 2017 decision on an

⁵⁷ For links to the papers and reports, see footnote 9, page 3 above.

⁵⁸ Regulation 2016/679 of the EU Parliament and Council of 27 April 2016 - <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

⁵⁹ <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

⁶⁰ See further '*ICO GDPR guidance: Contracts and liabilities between controllers and processors*' – draft for consultation', September 2017 - <https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf> and the EU Article 29 Working Party's, '*Opinion*



agreement between the Royal Free Hospital and Google DeepMind.⁶¹ 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 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 2018⁶², which found (at paragraph 20.7) that the agreement had properly characterised DeepMind as a data processor not a controller and observed (at paragraph 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?

AI projects: anonymization as a compliance tool. Whilst processing personal data to anonymise it is within the GDPR (because that processing starts with personal data), properly anonymized data is outside the GDPR as it is no longer personal:

“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” (GDPR Recital 26).

Referring to its *Code of Practice on Anonymisation*⁶³, the ICO lists anonymisation at one of its six key recommendations for AI:

“Organisations should carefully consider whether the big data analytics to be undertaken actually requires the processing of personal data. Often, this will not be the case; in such circumstances organisations should use appropriate techniques to anonymise the personal data in the data set(s) before analysis.” (paragraph 218.1)

The ICO states that the risk of re-identification is the key criterion here:

1/2010 on the concepts of “controller” and “processor”, 16 February 2010- http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

⁶¹ ‘Royal Free – Google DeepMind trial failed to comply with data protection law’, ICO, 3 July 2017 <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/> See also ‘Google DeepMind and healthcare in an age of algorithm’, Powles and Hodson, published version from January 2017 - <https://www.repository.cam.ac.uk/bitstream/handle/1810/263693/Powles.pdf?sequence=1&isAllowed=y>

⁶² ‘Audit of the acute kidney injury detection system known as Streams’, Linklaters, 17 May 2018 – http://s3-eu-west-1.amazonaws.com/files.royalfree.nhs.uk/Reporting/Streams_Report.pdf

⁶³ ‘Anonymisation: managing data protection risk code of practice’, ICO, November 2012 - <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>



“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”. (paragraph 135)

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

- **privacy notices:** “organisations should be transparent about their processing of personal data ... in order to provide meaningful privacy notices”; (paragraph 218.2)⁶⁴
- **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”; (paragraph 218.3)⁶⁵
- **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 minimisation and data segregation”; (paragraph 218.4)⁶⁶
- **ethical principles:** “organisations should develop ethical principles to help reinforce key data protection principles”; (paragraph 218.5 - see **section E** 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” (paragraph 218.6).

AI projects: pseudonymization as a further compliance tool in research. AI and very large datasets will increasingly be used for data and other science research. Personal data processed for scientific research is covered by the 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 pseudonymization (caught by the 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”.

⁶⁴ See further ‘Your privacy notice checklist’, ICO - <https://ico.org.uk/media/for-organisations/documents/1625126/privacy-notice-checklist.pdf>

⁶⁵ See further ‘Data Protection Impact Assessments (DPIAs)’, ICO, 22 March 2018 - <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf>

⁶⁶ See further ‘Data protection by design and default’, ICO - <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>



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 GDPR compliance tool for scientific research, which has certain benefits such as:

- processing for science 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.⁶⁷ AI's ability to uncover hidden links in data about individuals and to predict individuals' preferences can bring it within the GDPR's regime for profiling and automated decision making, defined by Art. 4(4) as:

“any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, 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”.

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

- “(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- (b) is authorised by Union or Member State law to which the controller is subject and 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.”

⁶⁷ See also 'Guidelines on automated individual decision-making and Profiling for the purposes of the GDPR', Article 29 Working Party, 3 October 2017 - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053; 'Machine learning with Personal Data – Profiling, Decisions and the EU GDPR', Kamarinou, Millard and Singh, Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016, November 2016 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811##. In February 2018, the UK House of Commons Science and Technology Committee launched an inquiry into Algorithms in decision-making - <https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2015/algorithms-in-decision-making-inquiry-launch-16-17/>



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 therefore 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 the GDPR's requirements and the costs of human intervention in this way is likely to lead to claims about the quality and genuineness of the human decision making (although as AI develops, the quality of automated decision making will improve as well).

25. **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 relations with third parties (the principal) and the other of whom similarly manifests assent so to act or so acts pursuant to the manifestation."⁶⁸

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

26. **AI and contract law.** Commercial contracts for the development and use of B2B AI systems between developer/licensor/provider and licensee/customer will, in the short term, be broadly similar to other software contracts, whether provided on-premise as a licence or in-cloud as a service. Similar issues to those in software and data licences and agreements will need to be addressed in AI agreements and are not considered further here.⁶⁹ 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. Paragraph **C.19** above overviews contractual aspects from the standpoint of the developer, smart contract platform operator and user. 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

⁶⁸ *'Bowstead and Reynolds on Agency'*, 20th Edition, page 1, Sweet & Maxwell, 2016

⁶⁹ For further information on IT contracts generally see our white paper *'Demystifying IT Law'*, June 2018 - http://www.kempitlaw.com/wp-content/uploads/2018/06/Demystifying_IT-White-Paper-KITL-v3.0-June-2018.pdf and in relation to Cloud legal services, our blog *'Law Firms and Contracting for the Cloud'*, 15 October 2014, <http://www.kempitlaw.com/law-firms-and-contracting-for-the-cloud/>



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 uncertainty⁷⁰ 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 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.

27. **AI and intellectual property: software – works/inventions generated/implemented by computer.** AI will provide a significant impulse to the development of intellectual property law, particularly as machine learning, dynamic AI algorithms and deep neural networks start to enable computers to generate new works and invent novel ways of doing things.

Copyright. In the copyright area, UK law has always developed with new bits added on Lego-like as technology evolves.⁷¹ 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 1988⁷² (**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 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”, widespread use 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.

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

⁷⁰ See ‘*Chitty on Contracts*’, 32nd Edition, Sweet & Maxwell, paragraph 2-147

⁷¹ 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 the EU Directive 2001/29/EC on Copyright and Related Rights in the Information Society.

⁷² <http://www.legislation.gov.uk/ukpga/1988/48/contents>



patent application “relates to that thing as such”.⁷³ 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).⁷⁴

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) 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.

28. 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”.⁷⁵

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*⁷⁶ is generally taken as authority for the proposition that there is no property *in* data as it cannot be

⁷³https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/354942/patentsact19770110_14.pdf

⁷⁴ Starting with *Aerotel Ltd v Telco Holdings Ltd* and *Macrossan’s Patent Application* [2006] EWCA Civ 1371

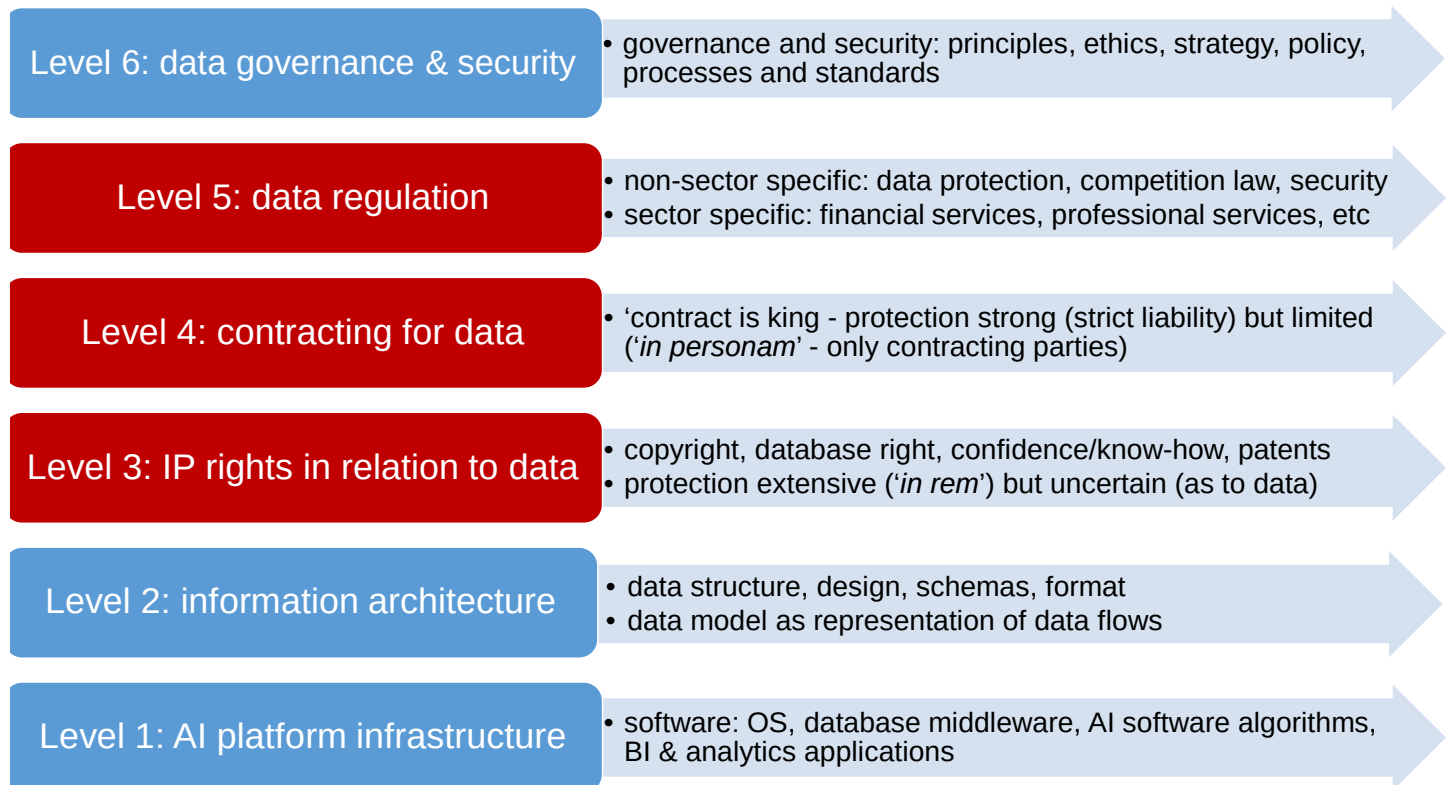
⁷⁵ See ISO/IEC Standard 2382:2015, IT – Vocabulary. See <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en>, terms 2121271 and 2121272. Information and data are used interchangeably here.

⁷⁶ [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



stolen; and the 2014 *Your Response*⁷⁷ 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.

Figure 6: Towards a common legal framework for data



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)⁷⁸. Current developments in each of these areas mean that 'data law' is emerging 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 three layers of a 6 layer stack, sandwiched between AI platform infrastructure and information architecture below and data ethics, governance and security above (see Figure 6 above, 'Towards a common legal framework for data').

⁷⁷ *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. See <http://www.bailii.org/ew/cases/EWCA/Civ/2014/281.html>. 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.

⁷⁸ For a more in-depth review of the technical aspects of data law see Kemp, 'Legal Aspects of Managing Big Data', October 2014 - <http://www.kempitlaw.com/wp-content/uploads/2014/10/Legal-Aspects-of-Big-Data-White-Paper-v2-1-October-2014.pdf> and Kemp et al, 'Legal Rights in Data' (27 CLSR [2], pp. 139-151).



Rights in relation to data: practical challenges. The April 2018 House of Lords report '*AI in the UK: ready, willing and able*' referred to above 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 ..'⁷⁹

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 program⁸⁰: that data is inherently boundaryless is not in principle incompatible with 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 there is no tangible property.

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

29. 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 likely to see the most important AI-influenced legal 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

⁷⁹ See footnote 14 above, paragraph 62 of their Lordships' report (page 28) and question 56.

⁸⁰ CDPA, s.3(1)(b) - <https://www.legislation.gov.uk/ukpga/1988/48/section/3>



regulatory backdrop. The UK AEVA 2018, 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.

‘Static’ and ‘mobile’ AI are likely to involve their providers and users in common law duties of care (negligence) and ‘mobile’ AI will in addition involve considerations of nuisance and escape (*Rylands v Fletcher*) liability.

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”⁸¹, 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.

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 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.”⁸²

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 ground⁸³. Extending *Rylands v Fletcher* escape liability in tort to AI would therefore appear to be a relatively simple extension consistent with past decisions.

⁸¹ Lord Macmillan in *Donoghue v Stevenson* [1932] A.C. 562 at p. 619.

⁸² (1866) L.R. 1 Ex. 265 at 279.

⁸³ 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. 108; cricket ball – *Bolton v Stone* [1951] A.C. 850.



E. AI IN THE ORGANISATION: ETHICS AND GOVERNANCE

30. **Introduction.** Broad recognition of AI's power to transform has led to a burgeoning in 2018 of reports, guidance and codes of conduct from government and AI industry stakeholders aiming to align their use and development of AI to ethical values and best practice. In the UK, and in addition to the reports referred to elsewhere in this paper, 2018 so far has seen:

- the DDCMS consult on the Centre for Data Ethics and Innovation (June to September);⁸⁴
- the DDCMS publish a Data Ethics Framework to “guide the appropriate use of data by public sector organisations to inform policy and design” (August);⁸⁵ and
- the Department of Health & Social Care (**DHSC**) publish an initial Code of Conduct for data-driven health and care technology (September).⁸⁶

31. **AI Governance - General.** Beginning with Open Source Software governance ten 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 recently received a boost in the area of data protection 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.

HM 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 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.⁸⁷

We suggest organisations may consider taking a similar approach in the area of AI and data ethics and follow the lead of large technology developers in the case of AI principles (paragraph **D.32**) and the UK Government for AI and data ethics policy and processes (paragraph **D.33**)

32. **AI Principles.** Both Microsoft and Google have published in 2018 a set of principles to guide AI development, and these are set out at Table 2 below. Although couched in different terms, they each seek to promote fairness, safety and reliability, privacy and security, inclusiveness, transparency and accountability. This could be a useful start point for the organisation's own statement of AI principles.

⁸⁴ <https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation>. The Centre for Data Ethics and Innovation was announced by the Chancellor in the Autumn Budget 2017 to address AI/data ethical and economic issues, develop best practice and advise on policy and regulation gaps.

⁸⁵ <https://www.gov.uk/government/publications/data-ethics-framework>

⁸⁶ <https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology>

⁸⁷ 'Legal Aspects of Cloud Computing: Cloud Security', paragraph C.19, Kemp, June 2018 - <http://www.kempitlaw.com/wp-content/uploads/2018/06/Cloud-Security-White-Paper-KITL-v1.0-June-2018.pdf>



Table 2 – AI Principles: Microsoft (January 2018) and Google (June 2018)

	Microsoft - Principles that should guide AI development ⁸⁸	Google - AI Principles ⁸⁹
1.	Fairness: AI systems should treat all people fairly	AI should avoid creating or reinforcing unfair bias
2.	Reliability and Safety: AI systems should work 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 by 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: of those who design and deploy AI systems	AI should be accountable to people
7.		AI should be made available for uses that accord with these principles

33. **AI governance – the UK Government’s Data Ethics Framework.** HM Government, as the steward of the country’s largest datasets, is also at the forefront of ethics, best practice and governance for AI.

In his foreword to the DDCMS Data Ethics Framework, the Minister states:

“Making better use of data offers huge benefits, in helping us provide the best possible services to the people we serve.

However, all new opportunities present new challenges. The pace of technology is changing so fast that we need to make sure we are constantly adapting our codes and standards. Those of us in the public sector need to lead the way.

As we set out to develop our National Data Strategy, getting the ethics right, particularly in the delivery of public services, is critical. To do this, it is essential that we agree collective standards and ethical frameworks.

Ethics and innovation are not mutually exclusive. Thinking carefully about how we use our data can help us be better at innovating when we use it.

Our new Data Ethics Framework sets out clear principles for how data should be used in the public sector. It will help us maximise the value of data whilst also setting the highest standards for transparency and accountability when building or buying new data technology.”

⁸⁸ ‘*The Future Computed: Artificial Intelligence and its Role in Society*’, Microsoft, January 2018, pages 57-74 - <https://news.microsoft.com/futurecomputed/>

⁸⁹ ‘*AI at Google: our principles*’, Sundar Pichai, Google CEO, June 7, 2018 - <https://www.blog.google/technology/ai/ai-principles/>. Google also espouses four ‘negative’ principles of AI design and deployment that it will not pursue. These are technologies (i) that cause overall harm, (ii) for weapons, etc, (iii) for surveillance that violate internationally accepted norms and (iv) that breach principles of international law and human rights.



This Framework published in June and updated to 30 August 2018) sets out seven principles and drills down from each to additional guidance. Table 3 sets out the principles and the areas of additional guidance.

We suggest the framework, with some adaptation, 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 form of workbook which it states should assist public sector teams record the ethical decisions they have taken about their projects.

Table 3: Summary of June 2018 UK Government Data Ethics Framework⁹⁰

Principle 1: Start with clear user need and business benefit. Using data in more innovative ways can transform service delivery. Always be clear about what we are trying to achieve for our customers.	
P1.1 Show how data can help meet user needs	P1.3 Determine business benefit
P1.2 Write up user needs	P1.4 Evidence correct understanding of problem
Principle 2: Be aware of relevant legislation and codes of practice. Understanding the relevant laws and codes of practice that relate to the use of data. When in doubt, consult relevant experts	
P2.1 Personal data	P2.6 Data protection by design
P2.2 Equality and discrimination	P2.7 Accountability
P2.3 Sharing and re-use of data	P2.8 Data minimisation
P2.4 Copyright and intellectual property	P2.9 Information governance
P2.5 Sector specific legislation	
Principle 3: Use data that is proportionate to the user need. Data use must be proportionate to the user need. Use the minimum data necessary to achieve the desired outcome	
P3.1 Personal data and proportionality	P3.4 Personal data and proportionality
P3.2 data source and proportionality	P3.5 Purposefully newly collected data
P3.3 Repurposed operational data	
Principle 4: Understand the limitations of the data. Data used to inform service design must be well understood. Consider the limitations of data when assessing if it is appropriate for a user need	
P4.1 Provenance	P4.3 Bias
P4.2 Errors	P4.4 Metadata and field names
Principle 5: Ensure robust practices and work within your skillset. Insights from new technology are only as good as the data and practices used to create them. Work within your skillset recognising where you do not have the skills or experience to use a particular approach or tool to a high standard	
P5.1 Multidisciplinary teams	P5.4 Social bias in algorithms
P5.2 Getting help from experts	P5.5 Reproducibility
P5.3 Accountability of algorithms	P5.6 Test the model

⁹⁰Data Ethics Framework, Guidance and Workbook, Department for Digital, Culture, Media & Sport, published June 13, 2018 as updated August 30, 2018 - <https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework>.

**Principle 6: Make your work transparent and be accountable.**

Be transparent about the tools, data and algorithms used for the work, and open where possible. This allows other researchers to scrutinise the findings and users to understand the new types of work being carried out.

P6.1 Good practice for making work transparent

P6.3 Share model for algorithmic accountability

P6.2 Sharing your data

P6.4 Algorithm transparency and interpretability

Principle 7: Embed data use responsibly.

There must be a plan to ensure insights from data are used responsibly. All teams must understand how findings and data models are to be used. They must be monitored with a robust evaluation plan.

P7.1 Designing/delivering services with data

P7.5 When to retrain/redesign a predictive model

P7.2 Ensuring appropriate knowledge and support when deploying to non-specialists

P7.6 Monitoring personalisation or tailored service delivery

P7.3 Monitor model efficacy post-deployment

P7.7 Algorithms in decision making

P7.4 Responsibility for ongoing maintenance

34. **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, and the ISO/IEC and other technical standards bodies are active on AI standardisation. ISO/IEC JTC (Joint Technical Committee) 1/WG (Working Group) 9 (on Big Data) has published in the 5-part standard 20547 (IT – Big Data) parts 2 (use cases) and 5 (standards roadmap). ISO/IEC JTC1 / SC (Sub-Committee) 42 on AI was established in October 2017 and is working on ISO/IEC 22989 (AI concepts and terminology) and ISO/IEC 23053 (framework for AI systems using machine learning). Organisations should keep abreast of standards development in the AI area so they when tendering for AI technology they can consider whether prospective providers can give the assurance provided by relevant technical standards.

F. CONCLUSION

35. **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 whose threshold we are now crossing. As AI develops, it may come to impact 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 short, medium and long term. Policy makers and regulators are consequently grappling with what AI means for law and policy and the necessary technical, legal and regulatory frameworks. 2018 has seen important policy announcements in the EU and the UK which herald a more 'joined up' approach to AI. 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, and developments in data protection, contract, intellectual property and tort law as the legislature make new statute law and as the courts decide disputes and make new case law. AI is already another fascinating area for IT lawyers.

Richard Kemp,
Kemp IT Law, London,
September 2018
richard.kemp@kempitlaw.com
Tel: 020 3011 1670



ANNEX 1 – EIGHT PRACTICAL HYPOTHETICAL SCENARIOS ILLUSTRATING THE LEGAL AND REGULATORY IMPACT OF AI (PARA C.20)

a) a car, ambulance and bus, all operating autonomously, collide at a road intersection

assumptions: autonomous vehicles operating on public roads without human supervision/physical presence is permitted by law (NB: this requires change to UK legal framework as at September 2018)

Legal actors	Legal and regulatory issues			
	A. Contract law	B. Tort law	C. Regulation	D. Other issues
1. Vehicle owner	- no contract between operators of different vehicles - chain/'ecosystem' of contracts between vehicle owner/operator – dealer (leasing co) – manufacturer – AI vendor (if not m'facturer) - provider will seek to get customer to acknowledge AI risk & to limit its liability & legal responsibility	- contracts will seek to exclude tort liability - negligence liability – duty of care owed? (✓?); establish breach on normal principles? - actionable breach of statutory duty? - m'facturer's strict liability (UK↓, USA↑)	- vehicle: AI to be tested, data recording. Data protection, data security, transition to human control, failure warning - road traffic law: (i) setting AI vehicle requirements; (ii) operators' duty to comply - liability of ambulance & bus operators & management - data protection, security and sovereignty issues - ownership of data generated	'black box' recording all data to be kept on board/in-cloud for all 3 vehicles to enable evidence-based determination of fault/liability - regulatory framework to ensure black boxes are installed, operated, maintained, etc - international regulatory framework update – Geneva/Vienna Road Traffic Conventions - in respect of the AIs used in the vehicles, standards as to (i) testing, acceptance & performance, (ii) APIs & communication - public sector standards for ambulance (assuming publicly operated, as in UK), bus (private company) car (private owner)
2. Vehicle operator				
3. Vehicle manufacturer				
4. Vehicle dealer				
5. AI vendor (if different)				
6. Insurers	- insurance contract required between each of actors 1-5 and insurance company? - scope of disclosure requirements & 'utmost good faith, (cp UK Insurance Act 2015)	-	who must carry insurance, for what risks & what liability minimum?	- de-mutualisation of insurance risk through AI/big data & treatment of marginal cases – risk of actionable discrimination? - evidence of testing/performance, etc of AIs as part of insurability evaluation? - how to price premiums for AI risks?
7. Highways authority	contractual arrangements where operations (e.g. AI-IT related) are outsourced	- actionable statutory duty? - limits of liability?	extend duty to functioning sensors (cp street lamps), etc?	- growing importance of (e.g.) ISO standards - how to address growing volume of sensors? - approach by State to AI where regulated: unitary/centralised agency or fragmented/sector/authority by authority approach?
8. Vehicle licensing authority			- testing of AI-enabled vehicles - see vehicle (1 to 5) above	



b) Multiple robots work with each other in the home

Legal actors	Legal and regulatory issues					
	A. Contract law	B. Tort law	C. Regulation	D. Other legal issues		
1. robot owner	- no contract between operators of different robots - chain of contracts between robot owner/operator/manufacturer/ AI vendor (if not m'facturer) - provider will seek to get consumer to acknowledge AI risk & to limit its liability & legal responsibility - Insure against all relevant risks	manage negligence, nuisance, 'escape' (<i>Rylands v Fletcher</i> in UK), safety & other tort liability of land owner/ lessee/occupier, etc – e.g. in contract & by insurance	consumer protection – (i) re user in the home in the even of accident caused by faultily operating robot either singly (vacuum cleaner injures owner) or together (vacuum cleaner and home sensing AI)	- Note common misconception that robots can be agents or have legal personality – robots are goods of their owner with no capacity for independent legal action - Data protection and security issues		
2. robot operator						
3. robot manufacturer		as above + manufacturers' (inc strict) liability				
4. AI vendor (if different)	see earlier slides					
5. Insurers	see earlier slides					
6. Standard setting organisations (e.g. ISO)	-	-	-	growing importance of (e.g.) ISO standards		
7. Regulatory authorities	contractual arrangements where operations (e.g. AI-IT related) are outsourced	- actionable statutory duty? - limits of liability?	- extend occupiers' liability to cover robot activities? - Liability for robot use outside the home?	- how to address growing volume of sensors? - approach by State to AI where regulated: centralised (more efficient?) or authority by authority approach?		



c) Separate smart contract systems incorrectly record a negotiated a loan agreement between lender and borrower

key assumption: legal framework permits use of AIs in the manner predicated

Legal actors	Legal and regulatory issues			
	A. Contract law	B. Tort law	C. Regulation	D. Other legal issues
1. Lender	• lender's (bank's) contract must get explicit from borrower explicit agreement to use of lender's AI, interaction with borrower's AI and scope of authority to negotiate (smart contract points) • ? Get signature from both parties	• contracts may be expected to seek to exclude all tort all other non-contractual liability where exclusion is possible • exclusion of liability for contract breach/tort/regulatory breach: • circumscribed in B2B contracts (UCTA, regy); • prohibited in B2C contracts?	• authorisation by regulators (FCA/ BoE in the UK) for: • (i) banking, (ii) selling, (iii) lending activities; • ?(iv) AI and (v) [blockchain] smart contract activities?	• note specific writing requirements for guarantees, mortgages (Statute of Frauds) and disposition of interests in land (LPA) • blockchain application? • data protection, security and sovereignty issues
2. Lender's AI vendor (if different)	• contract will seek to get binding AI performance commitments, etc & address risk/liability		• specific authorisation (FCA under FSMA) for lending-side AI?	• for the AIs used standards as to (i) testing, acceptance & performance, (ii) APIs & comms
3. Borrower's intermediary	• flip side of lender's points • limited negotiating power, regulatory redress (limited in B2B, extensive in B2C?)		• regulatory authorisation by FCA (under FSMA) for AI-enabled borrower intermediary	• discrimination claim risk where applicants turned down?
4. Borrower's [intermediary's] AI	• contract will seek to get binding AI performance commitments, etc & address risk/liability		• specific authorisation (FCA under FSMA) for borrowing-side AI?	• for the AIs used, standards as to (i) testing, acceptance & performance, (ii) APIs & comms
5. Borrower	• limited negotiating power, but regulatory redress • how does the borrower access AI – through intermediary?	-	• consumer borrower: regulatory redress for lender, borrower intermediary default, etc?	• intrusive degree of regulatory protection for consumers? • less in B2B borrowing?
6. Insurers	• insurance required for 1, 2, 7 (lender) 3, 4, 8 (borrower)	-	• lender, borrower intermediary insurance requirement?	• evidence of testing/performance, etc of AIs as part of evaluation?
7. Lender's regulator	-	-	• authorisation <i>a priori</i> of blockchain/AI activities + periodical renewal? • (In UK) compliance with FCA handbook, et	• approach of State to AI where regulated: centralised authority (more efficient) or sectoral approach?
8. Borrower's ombudsman	-	-		



d) Companies use their AIs in their logistics, supply and manufacturing chains

key assumption: legal framework does not outlaw use of AIs in the manner predicated at any level in the chain

Legal actors	Legal and regulatory issues			
	A. Contract law	B. Tort law	C. Regulation	D. Other legal issues
1. Chain participant	• chain/'ecosystem' of contracts between all participants • need to address dependencies, single point of failure, relief events, etc? • provider will seek to get customer to acknowledge AI risk & to limit its liability & legal responsibility	• contracts will seek to exclude tort liability • negligence liability – duty of care owed? (✓?); establish breach on normal principles? • actionable breach of statutory duty? • manufacturer's strict liability (UK↓, USA↑)	• liability exclusion less heavily circumscribed in B2B contracts	• international supply chains predicated on common legal & regulatory approach? • importance of (i) international standards, (ii) international transport conventions, etc • in logistics, consider mode of delivery (e.g. drones) & regulation • will the AIs interoperate, and if so how (APIs, standards compliance, etc)?
2. AI vendor (if different)	• contract will seek to get binding AI performance commitments, etc & address risk/liability		• specific authorisation for AI?	• for the AIs used standards as to (i) testing, acceptance & performance, (ii) APIs & comms • data protection, security and sovereignty issues • ownership of data generated
3. Insurers	• contracting/[regulatory?] requirement for insurance against usual risks to be carried at each level of the supply chain?			• what are AI usual risks? • question of de-mutualisation of insurance risk through AI/big data & treatment of marginal cases – risk of actionable discrimination? • implications of moving from traditional insurance regulation (top-down actuarial based risk calibration) to data-enabled bottom-up, data/fact-based risk calibration?
4. Regulatory authorities	-	-	• would using AI in this way require regulatory authorisation? • for products that are themselves regulated [e.g.. medical equipment] or operate in a regulated environment [e.g.. utilities)? • what form does regulation take?	• Importance of (e.g..) ISO standards [e.g.. consumer/business electronics] • approach of State to AI where regulated: unitary/centralised authority or fragmented/sector/authority by authority approach?



e) Construction companies use multiple autonomous machines to build an office block

key assumption: legal framework permits use of AIs in the manner predicated

Legal actors	Legal and regulatory issues			
	A. Contract law	B. Tort law	C. Regulation	D. Other legal issues
1. Site freehold owner/lessee	- residual contract law liability to be excluded as far as possible in contracts with developer, etc - insure against all relevant risks	Manage negligence, nuisance, ‘escape’ (Rylands v Fletcher in UK), safety & other tort liability of land owner/ lessee/occupier, etc – e.g. in contract & by insurance	assess & manage (contractually, by insurance, regulatory permissions, etc) all AI/autonomous related legal risks	
2. Vehicle owner/operator/ manufacturer/dealer	see illustration (a) re: autonomous cars colliding			
3. AI vendor (if different)				
4. Developer	if developer commissions autonomous machines, address all AI use risks in (upstream) contracts with vehicle owner, engineers, etc if advising on machines	Address same types of tort issues as for land owners, etc	assess & manage (contractually, by insurance, regulatory permissions, etc) all AI/autonomous related legal risks	- data protection, security and sovereignty issues - ownership of data generated
5. Architects/Engineers, etc	if use of autonomous machines fall within scope of engineers’/other professionals’ roles on the project, manage risks in contract with developer, etc and ensure PI & public liability insurance AI-based risks are covered			
6. Building contractor/sub-contractors	- development contract will be based on standard form (e.g. JCT, RIBA in UK) - ensure development contract adequately addresses all relevant AI risks			
7. Insurers	- see earlier slides (statutory/regulatory) insurance requirements for all AI/autonomous machine risks for all involved in the building project – i.e. 1, 2, 3, 4, 5, 6, 8			- need specialist understanding of relevant AI related usual risks - see also slide 1 re: autonomous cars colliding
8. Planning and building inspection authorities	see illustration (a) above (autonomous vehicles collide) re rows 7 and 8			



f) AI is used for the supply of transportation and services in smart cities

key assumption: legal framework permits use of AIs in the manner predicated

Legal actors	Legal and regulatory issues			
	A. Contract law	B. Tort law	C. Regulation	D. Other legal issues
1. Utilities providers	• chain/’ecosystem’ of contracts between all participants • need to address dependencies, single point of failure, relief events, etc? • provider will seek to get customer to acknowledge AI risk & to limit its liability & legal responsibility	• manage negligence, nuisance, ‘escape’ (<i>Rylands</i> v <i>Fletcher</i> in UK), safety & other tort liability of land in contract & by insurance	• will the provider’s obligations/ liability (low threshold of performance obligation in UK currently) be increased in the smart city context through use of AI? • data protection, security and sovereignty issues • ownership of data generated	• in the event of service failure caused by faulty AI, evidential difficulties of assessing who is at fault and therefore liable • requirement to retain data for [x?] years (‘black box’ basis) to enable assessment to be made? • expense and difficulty of disputes seeking to apportion blame & liability? • for the AIs used standards as to (i) testing, acceptance & performance, (ii) APIs & comms
2. Transportation provider				
3. AI vendor (if different)				
4. Insurers	• see earlier illustrations • (statutory/regulatory) insurance requirements for all AI risks for all involved in the utilities/transport services – i.e. 1, 2, 3 above			
5. Urban authority	-	-	• would using AI for these regulated service require regulatory authorisation? • what form does regulation take?	• approach of State to AI where regulated: centralised authority (more efficient?) or sectoral approach (urban, utilities, transportation?)
6. Utilities regulator	-	-		
7. Transportation regulator	-	-		



g) multiple AI-enabled satellites work with each other in space

Legal actors	Legal and regulatory issues			
	A. Contract law	B. Tort law	C. Regulation	D. Other legal issues
1. satellite owner	- no contract between operators of different satellites - chain of contracts between satellite owner/ operator/ manufacturer/ AI vendor (if not m'facturer) - provider will seek to get customer to acknowledge AI risk & to limit its liability & legal responsibility - insure against all relevant risks	manage negligence, nuisance, 'escape' (<i>Rylands</i> v <i>Fletcher</i> in UK), safety & other tort liability – e.g. in contract & by insurance	- statutory regulatory requirements to be complied with – e.g. in UK Outer Space Act 1986 - data protection, security and sovereignty issues - ownership of data generated	how far and to what extent does this happen at the moment?
2. satellite operator				
3. satellite manufacturer				
4. AI vendor (if different)	see earlier illustrations			
5. insurers	see earlier illustrations			
6. Regulator (UK Space Agency in UK)	-	-		international treaties/coordination, etc



h) medical and healthcare diagnostics and procedures are planned and carried out by and using AI and robotics

Legal actors	Legal and regulatory issues			
	A. Contract law	B. Tort law	C. Regulation	D. Other legal issues
1. Patients	impact of AI/robotics on (i) NHS & (ii) private patients expectations & standards	new areas of tort liability for AI/robotics use? (flipside of risk for providers at 2 – 6 below)	privacy, data sharing & access to electronic health records (EHRs)	- AI systems introduce new errors? - societal surveillance issues?
2. Clinicians	NHS/private - manage risk by contractual warranty, indemnity & liability terms	- further areas of tort liability - actionable data protection breaches	- patient privacy - AI impact on Medical Act 1983	monitoring/ being monitored burden
3. Pharmaceutical providers	manage contractual risk through warranty, indemnity & liability terms	- what extra areas of tort liability does use of AI/robotics, etc involve? - negligence, <i>Rylands v Fletcher</i> escape? - further areas of strict liability? Breach of statutory duty?	- Impact of AI on medicines and devices regulation - data protection issues sensitive data, reidentification risk from 'anonymised' data	- ethics, privacy & discrimination health care outcomes? - privacy, surveillance and ethical risks - DeepMind NHS renal & vision projects - IBM Watson health applications
4. Healthcare providers	manage contractual risk through warranty, indemnity & liability terms			
5. Bio/robotics/AI providers	- terms of use/risk/liability for robotic surgery/virtual avatars/companion robots - risks, etc e.g. of machine learning system to monitor for drug adherence - check liability terms carefully			
6. Insurers	address data protection implications in collecting customer data, etc		calibrate regulatory risk/liability as framework changes	- AI/big data demutualisation risk? - need to justify cross subsidisation?
7. Regulators	- negligence (duty of care) AI standards; escape/nuisance robotics standard - new standards for implantables, etc? - see Governments at 8.		- AI implications for regulation of doctors, etc, medicines and devices - policy framework: (i) preventing public harm & ensuring economic fairness; (ii)	
8. Governments	- establish licensing/provision framework and terms for outcome data, etc - establish policy frameworks for AI/machine learning use, robotics/implants, smart/implantable drug delivery mechanism, etc - note increasing importance of international standards - see regulators at 7.		- impact of big data on data protection – does most data tend towards personal data? - establishment of secure registries for outcome data - anonymisation techniques and efforts	



Annex 2 - Glossary of terms used

Acronym	Term	Where First Used
ADAS	Advanced Driver Assistance System	C.17
AEVA	Automated and Electric Vehicles Act 2018	C.17, footnote 44
AI	Artificial Intelligence	A.1
AlaaS	AI as a Service	C.14
AKI	Acute Kidney Injury	D.24
ANPR	Automated Number Plate Recognition	C.17
API	Application Programming Interface	C.14
ART	Automated Recognition Technologies	C.17
AVT	Automated Vehicle Technology	C.17
CAV	Connected and Autonomous Vehicles	C.16
CCAV	Centre for Connected and Autonomous Vehicles	C.17
CDPA	Copyright, Designs and Patent Act 1988	D.27
CLI	Command Line Interface	B.11
CPU	Central Processing Unit	B.9
CSP	Cloud Service Provider	B.7
DBEIS	Department for Business, Enterprise and Industrial Strategy	D.23
DDCMS	Department for Digital, Culture, Media & Sport	D.23
DfT	Department for Transport	C.17
DHSC	Department of Health & Social Care	E.30
DLT	Distributed Ledger Technology	C.18
Epoch	number of training data blocks	B.10, Figure 4
FCA	Financial Conduct Authority	C.15
GDPR	General Data Protection Regulation	D.24
GPS	Global Positioning System	C.16
GPU	Graphics processing Unit	A.3
GUI	Graphical User Interface	B.11
IMU	Inertial Measurement Unit	C.17
IPR	Intellectual Property Right	D.27
ICO	Information Commissioner's Office	C.17
ISO	International Organisation for Standardisation	A.2
LIDAR	L ight D etection A nd R anging	C.16
LSA	Legal Services Act 2007	C.15
LSB	Legal Services Board	C.15
LSP	Legal Services Provider	C.15
METI	Ministry of Economy, Trade and Industry (Japan)	A.5, footnote 9
MIIT	Ministry of Industry & Information Technology (China)	A.5, footnote 9
NLP	Natural Language Processing	A.3
PA	Patents Act 1977	D.27
PRA	Prudential Regulation Authority	C.15
Radar	R adio D etection A nd R anging	C.16
SRA	Solicitors Regulation Authority	C.15