AI in capital markets: Navigating legal and regulatory considerations

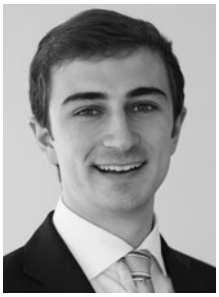
Received (in revised form): 9th May, 2022

Mike Pierides*
Partner, Morgan, Lewis & Bockius

James Mulligan**
Associate, Morgan, Lewis & Bockius

Christopher Archer***
Associate, Morgan, Lewis & Bockius

Mike Pierides



James Mulligan

Christopher Archer

Morgan, Lewis & Bockius LLP, Condor House, 5–10 St. Paul's Churchyard, London EC4M 8AL, UK

**Tel.: +44 20 3201 5686; E-mail: mike.pierides@morganlewis.com*
***Tel.: +44 20 3201 5496; E-mail: james.mulligan@morganlewis.com*
****Morgan, Lewis & Bockius LLP, 1701 Market St., Philadelphia, PA 19103-2921, USA Tel: +1 215-963-4966; E-mail: christopher.archer@morganlewis.com*

Journal of Securities Operations & Custody
Vol. 14, No. 4, pp. 299–313
Henry Stewart Publications
1753-1802

Mike Pierides *leads Morgan Lewis's Technology, Outsourcing and Commercial practice outside the US. His practice encompasses a wide breadth of commercial and technology transactions. Mike advises on major outsourcings, strategic restructurings following divestments or acquisitions and technology-specific transactions such as licensing and 'as a service' arrangements. He is also active advising on new technologies such as blockchain and artificial intelligence.*

James Mulligan *is an associate in Morgan Lewis's Technology, Outsourcing and Commercial practice. He advises clients on technology, cloud outsourcing and commercial transactions, including drafting and negotiating software licensing and resale, data processing, joint development and master services agreements. James regularly advises clients in highly regulated industries and has completed a secondment to a leading technology and financial services business, where he negotiated high-value outsourcing arrangements as part of corporate actions. James has a particular interest in advising on the use of new technologies, such as artificial intelligence, within financial services.*

Chris Archer *is a senior associate in Morgan Lewis's Technology, Outsourcing and Commercial practice. Chris focuses his practice on outsourcing, major technology and digital transformation initiatives, complex strategic commercial transactions, cloud services agreements, system implementation deals and other significant licensing agreements. As part of his role on these transactions, Chris manages complex deal structures, coordinates and leads diverse groups of stakeholders and manages various legal specialists. Chris works with clients on global outsourcing deals that span a wide range of business processes, including information technology, finance and accounting, procurement and other core and non-core functions. As a leader of deal teams, Chris oversees all aspects of transactions, which often require significant deal management and advice regarding scope of services, performance criteria, transition planning and implementation, security, privacy, intellectual property, liability, termination and wind down issues.*

Abstract

In capital markets, digitisation and cloud technology have catalysed opportunities for AI by enabling firms to collect, store and analyse larger datasets from a variety of internal sources than ever before. The past year brought greater regulatory activity around AI in the UK, EU and US than in any prior year, although regulatory regimes remain disparate. When considering legal issues that arise from use of AI, facets of multiple legal fields are relevant, albeit differing between jurisdictions, such as intellectual property rights frameworks and con-

tractual areas such as data ownership, data rights, risk and liability allocation and compliance responsibilities. In this paper, the key legal considerations and recent regulatory developments are categorised into four actionable, international themes: (i) due diligence of data as an asset; (ii) effective organisational ongoing controls; (iii) intellectual property management; and (iv) third party contract and risk management. With so much in flux, we find that the best approach for now is to consider such themes and ensure robust governance, transparency and explainability of each of the AI systems, human oversight of the AI and contractual arrangements with third party providers. Perhaps ironically, 'getting AI right' is currently, to a large extent, more an art of human judgement than any formulaic compliance with rules.

Keywords: artificial intelligence, machine learning, digitisation, financial regulation, legislation, intellectual property

According to a global 2021 survey, a significant proportion of corporates, possibly the majority, have adopted artificial intelligence (AI) in some form.[1] In capital markets specifically, digitisation and cloud technology have catalysed opportunities for AI by enabling firms to collect, store and analyse large datasets from a variety of internal sources, including trading desks, customer account history and communications, and external sources, including public filings and market data.[2]

Not surprisingly, given the increased business activity, the past year has brought greater regulatory activity around AI in the UK, EU and US than in any prior year. However, regulatory regimes remain disparate and use of AI is generally governed under activity-specific laws, such as algorithmic trading, data privacy and anti-discrimination laws.

While the most pertinent legal considerations for AI are currently in data rights ownership and ownership of intellectual property, regulatory considerations coming down the track are far-reaching and should be considered from now on; key themes include privacy issues, bias governance, transparency and trustworthiness of AI.

In this paper, two of the main types of AI used within securities operations and custody services are explored, along with example use cases. We then note certain legal considerations, take stock of recent transatlantic regulatory developments and, finally analyse certain practical legal and regulatory considerations raised by AI.

TYPES OF AI AND EXAMPLES WITHIN SECURITIES OPERATIONS AND CUSTODY SERVICES

AI refers to the 'capacity of computers or other machines to exhibit or simulate intelligent behaviour'.[3] This definition, from the Oxford English Dictionary, omits a 'human' aspiration of the machine's intelligence; by contrast, Merriam-Webster retains that human aspiration by defining AI as 'the capability of a machine to imitate intelligent human behavior'.[4] The difference belies an important point: the diverse umbrella of AI use cases and risks, together with varying levels of regulatory scrutiny, is to an extent attributable to the degree to which an AI system has complete or partial autonomous decision making, akin to human intelligence, or none at all.

Many AI solutions, such as those described in previous volumes of this journal, involve two technologies: robotic process automation (RPA) and machine learning.

Robotic process automation

This primarily refers to the use of pre-programmed software tools that interact with other applications to automate labour-intensive tasks, often resulting in increased accuracy, speed and cost-savings.[5] RPA can be seen as part of the incremental development of AI and can be an integral part of an

AI tool. Use cases could include digitalising submission and processing of withholding tax applications[6] and automating know-your-customer workflows.[7]

Machine learning (ML)

This primarily refers to the development of systems that can perform tasks as a result of a learning process that relies on data.[8] ML uses algorithms to process *and learn from* large amounts of input data in order to identify patterns or make predictions, rather than relying solely on embedded rules and statements within code. Use cases of ML within securities operations and custody services could include:

- optimising settlement orders through the AI system's ability to learn from interactions, both settlement fails and optimal transactions, and improve with time;[9]
- client segmentation in order to divide clients into discrete groups, which the AI system can itself identify, so that custodians can tailor products and services to meet the shared needs of client segments;[10]
- application in trade reconciliation to analyse historical breaks between trades or positions in order to identify reasons for future breaks and then attempt to resolve such breaks automatically;[11]
- transaction surveillance and conduct monitoring tools;[12] and
- risk management systems which visualise market risk by analysing trends, or liquidity risk by analysing multi-dimensional risk and exposure data.[13] Such systems might deploy 'Deep ML', which uses algorithms to process large amounts of unlabelled or unstructured data through multiple layers of learning that replicate how neural networks function in the brain.

While AI systems may simulate, imitate or even exhibit elements of human intelligence (as described in the definitions cited above), it is important for the purposes of transparency and accountability, among other reasons, to recognise the current technological limitations of AI systems. Artificial 'general' intelligence (AGI), the ability to learn intellectual tasks like humans, has not yet been achieved, and some leading academics suggest that AGI may not be realised before 2300.[14]

It is also important to note that AI systems used within capital markets are never a single solution or software program, but an ecosystem of clients and counterparties, intermediaries, cloud infrastructure providers, managed service providers, data service providers and third party advisers all providing input, review or relying on output. This is particularly important to note when considering practical issues of data, intellectual property rights, governance and transparency.

LEGAL ISSUES AROUND USE OF AI

When considering legal issues arising from the use of AI, facets of multiple legal fields are relevant, albeit differing between jurisdictions. These include intellectual property (IP) rights frameworks (ownership, licensing and infringement), product liability and contractual areas such as data ownership, data rights, risk and liability allocation, and compliance responsibilities. As with legal considerations in all software development and digital transformation, a 'ground-up' approach of end to end transformation and performance expectations is equally applicable to AI; technology contracts typically address technology development, transformation, enablement, acceptance, financial modelling, managing cost increases, key personnel, regulatory risks and changes, termination, information and audit, service levels and mechanisms for the contract itself to change as solutions or other terms evolve. Consideration of each of these issues

in relation to the development and use of an AI system will depend on the specific AI uses and ecosystems; analysis of these is beyond the scope of this paper. Such legal considerations when exploring certain key themes are considered below.

RECENT REGULATORY DEVELOPMENTS ON USE OF AI

Regulatory approaches to AI in the UK, EU and US are still in development, and at various stages of maturity, but all still fall short of the implementation of actual AI-specific legislation.

Given this state of flux, it is worth noting the risks and expectations in the use of AI by asset managers and market intermediaries that the International Organization of Securities Commissions (IOSCO), a global standard-setter for securities markets, published in September 2021.[15] These included:

- appropriate governance, controls and oversight frameworks over the development, testing, use and performance monitoring of AI;
- ensuring staff have adequate knowledge, skills and experience to implement, oversee and challenge the outcomes of AI tools;
- consistent and clearly defined development, testing and monitoring processes of algorithms, particularly ensuring that AI algorithms do not behave inexplicably owing to any subtle shift in operating conditions or excessive 'data noise';
- data quality and bias, ensuring the quality of sources used as well as the relevance and completeness of data; and
- appropriate transparency and explainability of algorithms, recognising the need to balance the necessary understanding by clients and regulators with the commercial sensitivity of the AI developer.

Where third party providers are used to provide AI systems or functions, IOSCO expects firms to have a clear service level agreement and contract in place that clarifies the scope of the outsourced AI functions and the service provider's responsibility. The agreement should contain clear key performance indicators and should also clearly determine suitable recourse for poor performance. IOSCO also highlights a risk of concentration of expertise in AI and of providers of the data used by AI; IOSCO's separate 'Principles on Outsourcing' provide guidance on addressing those potential risks.[16] As a global standard-setter, its findings may influence national regulators' developing approaches to AI regulation, and its expectations on asset managers could be flowed down to their providers of securities operations and custody services.

United Kingdom

In September 2021, the UK Government published its National AI Strategy, which detailed the government's ambition to drive AI innovation for the next 10 years.[17] As shown in Table 1, the National AI Strategy comprises various policies across government departments designed to ensure the UK gets the national and international governance of AI technologies right. As to a legislative approach, the UK Government's current position is that a blanket, AI-specific UK legislation would be inappropriate for four key reasons:

i. The boundaries of the potential harms of AI are grey.
ii. Use cases for AI have the potential to be highly complex.
iii. Empowering regulators and industries to respond and work with innovators in their sectors to advise on interpretation of existing regulations will enable a much faster response to individual harms.
iv. It may be difficult to differentiate between the specific impact of AI against other external factors, such as other ongoing technology changes.

Table 1 Summary of key actions, UK National AI Strategy

	Investing in the long-term needs of the AI ecosystem	Ensuring AI benefits all sectors and regions	Governing AI effectively
Short term (next 3 months):	• Publish a framework for the government's role in enabling better **data** availability in the wider economy • Consult on the role and options for a National **Cyber-Physical Infrastructure** Framework • Support the development of AI, data science and digital skills through the **Department for Education's Skills Bootcamps**	• Begin engagement on the Draft National Strategy for AI-driven technologies in **Health and Social Care**, through the NHS AI Lab • Publish the **Defence AI Strategy**, through the Ministry of Defence • Launch a **consultation on copyright and patents for AI** through the IPO	• Publish the CDEI **AI assurance** roadmap • Determine the role of data protection in wider AI governance following the **data: a new direction consultation** • Publish details of the **approaches the Ministry of Defence will use when adopting and using AI** • Develop an **all-of-government approach to international AI activity**
Medium term (next 6 months):	• Publish research into what **skills** are needed to enable employees to use AI in a business setting and identify how national skills provision can meet those needs • Evaluate the **private funding** needs and challenges of AI scaleups • Support the National Centre for Computing Education to ensure **AI programmes for schools** are accessible • **Support a broader range of people to enter AI-related jobs** by ensuring career pathways highlight opportunities to work with or develop AI • Implement the **US UK Declaration on Cooperation in AI R&D** • Publish a **review** into the UK's computer capacity needs to support AI innovation, commercialisation and deployment • Roll **out new visa regimes** to attract the world's best AI talent to the UK	• Publish research into opportunities to encourage **diffusion of AI** across the economy • Consider how **Innovation Missions** include AI capabilities and promote ambitious mission-based cooperation through bilateral and multilateral efforts • Extend UK aid to support local innovation in developing countries • Build an open **repository of AI challenges** with real-world applications	• Publish white paper on a pro-innovation national position on **governing and regulating** AI • Complete an in-depth analysis on **algorithmic transparency**, with a view to developing a cross-government standard • Pilot an **AI Standards** Hub to coordinate UK engagement in AI standardisation globally • Establish medium and long-term horizon scanning functions to **increase government's awareness of AI safety**
Long term (next 12 months and beyond):	• Undertake a review of our international and domestic approach to **semiconductor supply chains** • Consider what **open and machine-readable government datasets** can be published for AI models • Launch a new **National AI Research and Innovation Programme** that will align funding programmes across UKRI and support the wider ecosystem • **Work with global partners on shared R&D challenges**, leveraging Overseas Development Assistance to put AI at the heart of partnerships worldwide • **Back diversity in AI** by continuing existing interventions across top talent; PhDs, AI and Data Science Conversion Courses and Industrial Funded Masters • Monitor and use the National Security and Investment Act to protect **national security** while keeping the UK open for business • **Include trade deal provisions in emerging technologies**, including AI	• Launch joint office for AI/UKRI programme to stimulate the development and **adoption of** AI technologies in high potential, lower AI maturity sectors • Continue supporting the development of capabilities around **trustworthiness, adoptability and transparency** of AI technologies through the National AI Research and Innovation Programme • Join up across government to identify where **using AI can provide a catalytic contribution to strategic challenges**	• Explore with stakeholders the development of an AI **technical standards engagement** toolkit to support the AI ecosystem to engage in the global AI standardisation landscape • Work with partners in multilateral and multi-stakeholder fora, and invest in **GPAI** to shape and support **AI governance** in line with UK values and priorities • Work with The Alan Turing Institute to **update guidance on AI ethics and safety in the public sector** • Work with national security, defence and leading researchers to **understand what public sector actions can safely advance AI and mitigate catastrophic risks**

The UK Government's Plan for Digital Regulation,[18] published in July 2021, includes an approach to regulating AI technologies across all sectors based on the following principles: (i) actively promoting innovation by seeking to remove unnecessary regulations and burdens and initially considering non-regulatory measures like technical standards to reduce burdens; (ii) achieving forward-looking coherent outcomes through a collaborative approach between regulators and businesses, as well as by making space for businesses to test and trial new business models, products and approaches; and (iii) exploiting opportunities and addressing challenges in the international arena, particularly through international regulatory cooperation, in order to facilitate international interoperability. These principles, although ostensibly welcome, are so far light on detail. The plan does however highlight key concerns for regulating AI to include the oversight, accountability and verification of content and transparency and use of advanced data analytics and algorithms. In January 2022, the UK Government announced a new AI Standards Hub, as of the National AI Strategy, in order to coordinate UK engagement in AI standardisation globally and particularly around the governance of AI.[19]

AI assurance is another priority in the National AI Strategy. Broadly, this means assessing and demonstrating the trustworthiness and efficacy of AI systems and could involve audit, performance testing, undertaking impact assessments of compliance with regulations, and assessing open-ended risks. On 8th December, 2021, the UK Centre for Data Ethics and Innovation (CDEI) published a roadmap towards building an effective ecosystem of AI assurance.[20] While the detail of the AI assurance roadmap is beyond the scope of this paper, it is worth noting the CDEI's suggestion that compliance with assurance mechanisms may, in the international regulatory context, enable presumptions of conformity and interoperability between different regulatory regimes; this could facilitate use of AI systems within global operating models. To the extent that an AI system processes personal data, the UK Information Commissioner's Office (ICO) has published guidance on best practices for auditing AI and complying with data protection laws, which the CDEI supports.[21] The ICO's guidance focuses on accountability and governance, fair, lawful and transparent processing, data security and compliance with individual rights. The ICO has also published standalone guidance on the explainability of AI systems for compliance with data subjects' rights.[22]

For financial services specifically, in February 2022, the Financial Conduct Authority (FCA) and Bank of England (BoE) published their final report following the UK Artificial Intelligence Public-Private Forum. The report highlighted concern around, among other matters, governance and accountability (including individual accountability under the Senior Managers & Certification Regime (SM&CR)) where firms take decisions using data-based or algorithmic methods.[23] As to what differentiates governance of AI from other emerging technologies, it was suggested to be 'the incremental capacity for autonomous decision-making, which means AI can limit or even potentially eliminate human judgement and oversight from key decisions', which challenges concepts of individual and collective accountability and enterprise-wide risk management. The changing role of data in the AI lifecycle also challenges organisations to be able to adapt their governance structures and AI-specific data standards over time. Data quality, the complexity of AI models (of inputs, variables, algorithms and outputs) and explainability were other key themes in the report. The

FCA will publish a discussion paper later in 2022 on issues around AI for which it is considering making rules or setting out expectations.

Where third party providers are used to provide AI systems or functions, firms should remember to assess any use of third party AI against the FCA's and/or the Prudential Regulation Authority's (PRA's) requirements on third party risk management and operational resilience, both published in March 2021.[24,25] The applicability of these requirements are specific to each arrangement, and so they are not summarised here.

One final area worth mentioning is the UK's IP framework. In March 2021, the UK Government called for views on adapting this framework to include intellectual property rights created by or using AI and found that responses differed on whether and how works or inventions created by AI should be protected, although there was consensus that AI solutions themselves should not own intellectual property rights (particularly given that AGI has not yet been achieved).[26] Until January 2022, the UK Government was consulting on reforming copyright protection of 'computer-generated works', which are works generated by a computer for which the author is the person by whom the arrangements necessary for the creation of the work are undertaken. The UK is one of the few countries that protects works generated by a computer where there is no direct human creator. Copyright protection for computer-generated works currently lasts for 50 years, and the UK Government is considering reducing this duration. The UK Government is also considering broadening the exception to copyright licensing of 'text and data mining' in order to potentially allow the mining of data for commercial research and databases, without requiring a licence.[27]

European Union

In contrast to the UK, the EU is proposing a comprehensive legislative approach to AI. In April 2021, the European Commission published its much-anticipated, EU-wide legislation for regulating AI (EU AI Regulation).[28] The EU AI Regulation categorises AI systems by risk profile based on their intended use and their function. 'High-risk' AI systems are those intended to be used as a safety component of products that are subject to third party ex ante conformity assessments or other standalone AI systems with an intended use that is specified in Annex III of the EU AI Regulation, including AI systems intended to be used for recruitment processes, or to evaluate individuals' creditworthiness. These AI systems would attract more onerous obligations covering, among other areas, data governance, documentation and record keeping, transparency, human oversight, accuracy and security. However, most of the use cases of AI solutions for securities operations and custody services, and other business to business uses within capital markets, are unlikely to fall within 'high risk'. Other AI systems such as chatbots would be subject to transparency obligations to ensure that users are aware that they are interacting with a machine, and manufacturers of non-high-risk AI systems would be able to self-regulate via non-binding codes of conduct.

The EU AI Regulation would have extra-territorial effect, applying to providers established inside or outside the EU and making available an AI system on the EU market or supplying for first use within the EU market, or where the output produced by the AI system is used within the EU (which would capture offshoring). The definitions of the regulation are such that a regulated financial institution deploying an AI solution would almost certainly be defined itself as a provider, or in any event as a user of an AI solution and therefore

subject to various rules within the regulations. The EU AI Regulation would be supervised by national authorities and a new European Artificial Intelligence Board would be established to facilitate implementation of the new rules. For breaches, heavy fines of up to the greater of €30m or 6 per cent of worldwide turnover are proposed.

The EU AI Regulation is, at the time of writing, being considered by the European Parliament and EU Member States. EU financial services regulators have fed into the development of the EU AI Regulation, as have the European Data Protection Board and European Data Protection Supervisor, and so little agency-specific indications of their regulatory approaches are available. Material issues are being considered by the consultation, not least the very definition of AI, with participants in the financial services sector concerned that the breadth of the definition will capture software and technology that has been deployed for many years, and arguably should not be subject to new or greater regulation.

As noted for the UK, users of AI within financial services in the EU should also assess whether any aspect of the use of AI falls within the European Securities and Markets Authority's guidelines on outsourcing to cloud service providers[29] or the European Banking Authority's guidelines on outsourcing arrangements,[30] as applicable.

United States

In the US, the federal regulatory approach to AI has largely been a cross-application of agency guidance and activity-specific rules, such as data privacy, intellectual property, product liability and anti-discrimination laws. Although there is currently no comprehensive federal regulation of AI, recent trends suggest that such a regulation is on the way. For instance, the Stanford 2022 AI Index found that the current 117th Congress is on track to record the greatest number of AI-related mentions since 2001, and more than triple that of the 115th Congress.[31]

Activity at the federal level has mostly involved information-gathering and establishing structures for advising on AI regulation. In April 2022, the Biden administration appointed 27 members to its new National Artificial Intelligence Advisory Committee to advise the federal government on a range of AI-related matters and issues, including providing recommendations on the current state of US AI competitiveness; the state of science around AI; issues related to the AI workforce, including barriers to employment supporting opportunities for historically under-represented populations; opportunities for international cooperation; and issues related to accountability and legal rights.[32]

In December 2021, the National Institute of Standards and Technology published a concept paper on an AI Risk Management Framework (RMF) that is 'intended for voluntary use and to address risks in the design, development, use, and evaluation of AI products, services, and systems'.[33] Among other points, the RMF emphasises the multitude of stakeholders within the AI ecosystem including designers, developers, users and implementers, evaluators and those responsible for governance, as well as individuals who could experience harmful effects of AI. Trustworthiness of AI systems is a key theme in the concept paper, and advancing 'trustworthy AI' was also at the centre of the EU-US Trade and Technology Council's inaugural joint statement in September 2021. This statement expressed both sides' intention to discuss measurement and evaluation tools and activities to assess the technical requirements for trustworthy AI, concerning, for example, accuracy and bias mitigation.[34]

Several US regulatory bodies have issued guidance on the use of AI. In June 2020, the Financial Industry Regulatory Authority

(FINRA) published a much-cited report that summarises the use of AI in the securities industry and provides guidance to firms.[35] FINRA flags AI-related risks of data bias and governance, outsourcing risks in key areas like financial crime monitoring and trade surveillance, as well as vendor management considerations such as requiring vendors to notify firms in the event of a security breach and giving firms the right to audit AI vendors. On bias in particular, the Federal Trade Commission (FTC) warned in an April 2021 blog post of the risks of racial or gender bias reflected in AI data sets and algorithms, and indicated that failure to address these results may lead to 'deception, discrimination . . . .and an FTC law enforcement action'.[36] The FTC expects transparency with business customers and consumers alike as to what an AI algorithm can achieve, supported by evidence, and how users' data is used.

US financial institutions should also be cognisant, when engaging third party AI providers, of compliance with broader operational resilience guidance. This includes the US federal banking regulators' (Federal Reserve, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation) consolidated guidance in October 2020, which was intended as a holistic framework and approach to operational resilience, including enterprise-wide risk management, business continuity management and third party risk management. Use of AI should be considered within such risk management frameworks where the AI use case could expose the institution to sufficiently high operational risk.

ADDRESSING LEGAL AND REGULATORY CONSIDERATIONS

Given the nascent status of regulatory developments and their fragmented nature, it may seem challenging to identify a starting point for addressing them.

Corporate governance structures have not yet been adapted to address these issues holistically and the structural response of the industry to these challenges will be an area to watch over the next few years. Relevant functions will include information technology, information security, legal and compliance, whose collaboration will be required to create upfront policies, procedures, terms and conditions and so on, implementing and maintaining an ongoing oversight programme of AI implementation, as well as responding to incidents and issues as they arise.

Regulatory bodies are also highlighting the importance of appropriate governance. For example, FINRA identifies that firms may find it beneficial to establish a cross-disciplinary technology governance group to oversee the development, testing and implementation of AI-based applications. The FCA and BoE suggest, amongst other activities, the establishment of an ethics framework.

From a substantive perspective, it is helpful to categorise the issues into four, actionable themes that underpin the key legal considerations and recent regulatory developments: (i) due diligence of data as an asset; (ii) effective organisational ongoing controls; (iii) intellectual property management; and (iv) third party contract and risk management.

These themes are discussed below, combining both legal and regulatory considerations. They are by no means exhaustive.

Due diligence of data as an asset. Data usage rights may pose the greatest practical legal challenge to developing and implementing an AI system. Datasets could be sourced internally by the customer, which is commonly the basis of a collaboration with an AI developer, or datasets could be purchased from third parties or extracted from market data. Taking the use case of optimising settlement processes, an organisation might consider: (i) which

transactional data points are required to train the AI system; (ii) whether such data comes from the customer, counterparty or third party data; (iii) if any transaction data is extracted from third party software, eg trade execution software; and (iv) whether a licence is required and, if so, if that licence allows the use of the data for training other software. It is critical to perform diligence on any purchased data to ensure no additional third party consents are required and to check for any restrictions on deriving conclusions or creating derivative works from such data for commercial use. It will be interesting to monitor the UK's review of reforms to intellectual property rights (in particular copyright and database rights) in this regard.

Considering regulatory expectations, a variety of data sources would ideally be used in order to avoid, or at the very least mitigate, bias outputs. As IOSCO notes, firms should be cognisant that datasets concentrated in a small number of providers could pose an outsourcing risk and a risk of data bias in the AI system.

If datasets include personal data, it is important to ensure that appropriate legal bases for processing are in place (which may include ensuring data subjects have provided sufficient consent for use of their data within the AI solution) or, if data is acquired from a third party, that the vendor represents that the personal data can be used for the intended processing in compliance with data protection laws; consider if indemnity protection is appropriate. If the processing of personal data is particularly high risk or of a significant volume, a specific data privacy impact assessment may need to be undertaken to assess and document whether the processing will comply data protection laws. In the UK, the ICO indicates that consent may be the most appropriate lawful basis for processing — even if performance of a contract is the basis for *use* of an AI system processing an individual's personal data, the ICO states that it may not be an appropriate ground for processing personal data to *develop* an AI system if that system can perform well enough without being trained on the individual's personal data, as these are separate forms of processing. Of course, reliance on consent would require greater transparency in the layers of training and processing within AI (if it is even possible, eg in Deep ML) in order to comply with any withdrawal of consent. This could involve non-negligible costs that the parties must agree.

Ongoing controls. Robust governance measures, accountability, trustworthiness and transparency are common principles from regulatory developments over the past year, feeding down from the Organisation for Economic Co-operation and Development's AI Principles.[37] Ensuring internally that AI outputs are accurate and conclusions are evaluated critically with human judgement is important to enable individual and collective accountability under existing governance frameworks, such as the UK SM&CR. As noted above, the complete elimination of human judgement through AGI is not yet a realistic consideration. For structuring governance frameworks, the FCA and BoE suggest that central governance functions may be appropriate for defining and enforcing standards along with the monitoring of AI, which it characterises as a 'second line of defence'. With third party providers, IOSCO suggests that contractual relationships include regular monitoring of performance and outputs, both internally and with the provider.

As to governing the use of data, the FCA and PRA suggest adapting current governance frameworks in two ways to accommodate AI use:

i. data governance frameworks need to consider how AI will be used alongside data and understand the impact when approving datasets; and

ii. cloud governance frameworks need to understand AI tools used on the cloud platforms and whether they are built in-house or provided by third parties as part of the cloud services.

In its RMF concept paper, the US National Institute of Standards and Technology highlights that risk-management processes should take account of the 'ecosystem' of AI, particularly as part of any resilience planning in a failure of the AI system. In the UK this would be a consideration for remediation planning, which is expected by the FCA and PRA. For example, if settlement processes were to become reliant on the efficiency of the outputs of an AI system, firms may need to nonetheless maintain channels to various counterparties to implement manual processes at short notice if the AI system were to fail.

Along the value chain, organisations may seek both transparency and assurance controls of how AI decision making impacts their services and the potential consequences of errors. Transparency is a legal consideration common to all software development and digital transformation; for AI, it is a pinch point of legal and regulatory considerations. FINRA suggests that firms require AI developers and users to provide a written explanation of the key input factors and the rationale attributed to the outputs. An FCA-commissioned report published in June 2021 highlights the importance of: (i) 'system transparency' relating to the operational logic (ie 'inner workings') of a given AI system; and (ii) 'process transparency' of an AI system's design, development and deployment (eg data management, quality assurance, training).[38] Contractual obligations on providers to generate and maintain service records in sufficient volume to provide this transparency is particularly important for applications of AI in financial services, where an AI system might analyse significant volumes of financial transactions. Cooperation with regulators and customers in order to explain elements of AI systems will likely be essential moving forward. Audit rights are important for transparency and governance, as is reporting, but consider if it is possible to audit the full spectrum of technology incorporated in the AI solution; it may need to be clear within contracts what may be audited and when — ie a service provider's AI development and training team, implementation team and then its lines of defence. Of course, the ability to audit the various levels of AI may be subject to the scope of rights in any data that is acquired.

Intellectual property management. As with legal considerations in all software development, it is important to document the taxonomy of IP rights in the solution, both pre-existing IP incorporated in the AI system and developed IP. For ML in particular, the ownership of any developed IP may be extremely valuable; a customer may seek ownership of process know-how and all outputs, while a developer will want to protect ownership of developments in the ML algorithm and any software arising from the solutions learning method. Where any customer pre-existing IP is incorporated in developed IP as part of a collaboration, this could affect the ability of the provider to offer a developed solution to other customers.

It is important from both a legal and regulatory perspective to consider licensing arrangements in the event of exit from an AI tool, whether planned or sudden, in order to minimise service disruption. Exit considerations are highlighted by IOSCO's report and in European regulators' guidelines on outsourcing and operational resilience. If moving to a new software or algorithm, customers of RPA tools may, for example, seek a continued right to use certain settings, preferences and methods, which could involve a mixture of owned rights and licensed rights in the original

RPA solution. The retention and portability of data analytics from an ML tool could be a key commercial consideration and may also be expected by regulators as part of resilience planning; for example, the historic trends, risks and exposure analytics from an ML-based risk management tool may need to be retained for record-keeping purposes. Ultimately, the customer's continued use of aspects of the AI tool could be a trade-off for the provider's ability to offer a developed solution, incorporating certain customer pre-existing IP, to its other customers.

Another legal consideration is to ensure, or to obtain, sufficient rights of interoperability and integration between the AI system and any legacy systems or applications that interact with the AI system. For legacy systems, this may be a point of diligence and obtaining necessary consents as noted above. For example, RPA tools may overlay other applications to automate processes, such as digitalising withdrawal tax application processing and automating know your customer checks. ML tools could be more intrusive, if intended to integrate or modify any settings of the other software in order to gain efficiencies and it is important to understand at any request for proposal or planning stage what will be involved.

Third party contract and risk management. Given the evolving layers of AI regulation, the contractual allocation of compliance responsibility within the AI ecosystem will become increasingly important. Broadly, if the logic/algorithm is trained on:

- supplier-provided data or a mixture of customer data and supplier data, it may make sense for the supplier to bear responsibility for compliance; or
- solely the customers' data, the customer might bear compliance responsibility.

The contractual allocation of other potential liabilities and risks (possibly along similar lines to the above), the scope of covered losses and any separate-track liabilities can be critical for managing AI-specific third party risks. These risks include loss of data, breach of compliance obligations and any regulatory fines, data protection claims, third party claims of IP infringement and reputational issues. Insurance coverage could mitigate at least some of these risks, although AI-specific coverage is still nascent. With so much uncertainty around the evolution of these risks and what compliance will require, the detail of allocations and any associated dispute escalation and resolution mechanisms may prove critical.

CONCLUDING REMARKS

As legal considerations and regulatory approaches to AI in the UK, EU and US are still evolving, the best approach for now is to consider and navigate certain key, international themes and ensure robust governance, transparency and explainability of each AI system, human oversight of the AI and contractual arrangements with third party providers. Perhaps ironically, 'getting AI right' is currently, to a large extent, more an art of human judgement than any formulaic compliance with rules.

REFERENCES

(1) McKinsey (2021) 'State of AI in 2021', McKinsey, available at www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2021 (accessed 29th July, 2022).
(2) Financial Industry Regulatory Authority (2020) 'Report on Artificial Intelligence in the Securities Industry', p. 1, FINRA, avail-

able at www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf (accessed 29th July, 2022).
(3) 'Artificial Intelligence' in 'Oxford English Dictionary', available at www.oed.com/viewdictionaryentry/Entry/271625 (accessed 29th July, 2022).
(4) 'Artificial Intelligence', Merriam-Webster, available at www.merriam-webster.com/dictionary/artificial%20intelligence (accessed 29th July, 2022).
(5) Financial Industry Regulatory Authority, p. 4, ref 2 above.
(6) Giralt, M. (2020) 'Why the Experience of COVID-19 will Accelerate Progress Towards Digitalisation and Automation', *Journal of Securities Operations & Custody*, Vol. 13, No. 1, pp. 5–12.
(7) Ray, A. (2019) 'Intelligent Automation: A New Frontier in Capital Markets Operations', *Journal of Securities Operations & Custody*, Vol. 12, No. 3, pp. 266–77.
(8) Ostmann, F. and Dorobantu, C. (2021) 'AI in Financial Services', The Alan Turing Institute, available at www.turing.ac.uk/sites/default/files/2021-06/ati_ai_in_financial_services_lores.pdf (accessed 29th July, 2022).
(9) Brownlee, T., Sommerfeld J. and Hansen, K. (2019) 'How AI is Changing Operations: From Settlement Optimisation to Automating Risk Monitoring', *Journal of Securities Operations & Custody*, Vol. 12, No. 2, pp. 102–15.
(10) Deutsche Bank (2021) 'Unleashing the Potential of AI in Securities Services', p. 7, available at https://corporates.db.com/files/documents/publications/DB_AI-Securities-Services_24pp_Web.pdf (accessed 29th July, 2022).
(11) Ray, ref 7 above.
(12) Financial Industry Regulatory Authority, p. 3, ref 2 above.
(13) International Organization of Securities Commissions (2021) 'The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers', available at www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf (accessed 29th July, 2022).
(14) Brooks, R. (2019) 'AGI has been Delayed', available at https://rodneybrooks.com/agi-has-been-delayed/ (accessed 29th July, 2022).
(15) International Organization of Securities Commissions, ref 13 above.
(16) IOSCO (2021) 'Principles on Outsourcing', available at www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf (accessed 29th July, 2022).
(17) HM Government (2021) 'National AI Strategy', available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf (accessed 29th July, 2022).
(18) Department for Culture, Media and Sport (2021) 'Digital Regulation: Driving Growth and Unlocking Innovation', available at: www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation/digital-regulation-driving-growth-and-unlocking-innovation (accessed 29th July, 2022).
(19) Department for Culture, Media and Sport (2022) 'New UK Initiative to Shape Global Standards for Artificial Intelligence', available at www.gov.uk/government/news/new-uk-initiative-to-shape-global-standards-for-artificial-intelligence (accessed 29th July, 2022).
(20) CDEI (2021) 'The Roadmap to an Effective AI Assurance Ecosystem', available at www.gov.uk/government/publications/the-roadmap-to-an-effective-ai-assurance-ecosystem/the-roadmap-to-an-effective-ai-assurance-ecosystem-extended-version (accessed 29th July, 2022).
(21) ICO 'Executive Summary', available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/executive-summary/ (accessed 29th July, 2022).
(22) ICO 'Explaining Decisions Made with AI', available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made

-with-artificial-intelligence/ (accessed 29th July, 2022).
(23) Bank of England (2022) 'Artificial Intelligence Public-Private Forum: Final Report', available at www.bankofengland.co.uk/research/fintech/ai-public-private-forum (accessed 29th July, 2022).
(24) Financial Conduct Authority (2021) 'PS21/3 Building Operational Resilience', FCA, available at www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf (accessed 29th July, 2022).
(25) Prudential Regulation Authority (2021) 'SS2/21 Outsourcing and Third Party Risk Management', available at www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343 (accessed 29th July, 2022).
(26) UK Intellectual Property Office (2021) 'Government Response to Call for Views on Artificial Intelligence and Intellectual Property', available at: www.gov.uk/government/consultations/artificial-intelligence-and-intellectual-property-call-for-views/government-response-to-call-for-views-on-artificial-intelligence-and-intellectual-property (accessed 29th July, 2022).
(27) UK Intellectual Property Office (2021) 'Artificial Intelligence and Intellectual Property: Copyright and Patents', available at www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/artificial-intelligence-and-intellectual-property-copyright-and-patents (accessed 29th July, 2022).
(28) European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts', available at https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed 29th July, 2022).
(29) European Securities and Markets Authority (2021) 'Guidelines on Outsourcing to Cloud Service Providers', ESMA, available at www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines.pdf (accessed 29th July, 2022).
(30) European Banking Authority (2019) 'Final Report on EBA Guidelines on Outsourcing Arrangements', EBA, available at www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1 (accessed 29th July, 2022).
(31) Stanford University (2022) 'The Artificial Intelligence Index 2022', Stanford University, available at https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf (accessed 29th July, 2022).
(32) US Department of Commerce (2022) 'Press Release, U.S. Department of Commerce Appoints 27 Members to National AI Advisory Committee', available at www.commerce.gov/news/press-releases/2022/04/us-department-commerce-appoints-27-members-national-ai-advisory (accessed 29th July, 2022).
(33) NIST (2021) 'AI Risk Management Framework Concept Paper', available at: www.nist.gov/system/files/documents/2021/12/14/AI%20RMF%20Concept%20Paper_13Dec2021_posted.pdf (accessed 29th July, 2022).
(34) U.S.–EU Trade and Technology Council (2021) 'U.S.–EU Trade and Technology Council, Inaugural Joint Statement', The White House, available at www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/ (accessed 29th July, 2022).

(35) Financial Industry Regulatory Authority, ref 2 above.
(36) Jillson, E. (2021) 'Aiming for Truth, Fairness and Equity in your Company's Use of AI', FTC, available at www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (accessed 29th July, 2022).
(37) OECD (2019) 'Recommendation of the Council on Artificial Intelligence', available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed 29th July, 2022).
(38) Ostmann and Dorobantu, pp. 45–64, ref 8 above.