

Written Evidence Submitted by Burges Salmon LLP

(GAI0064)

Burges Salmon LLP is a law firm which regularly advises clients on emerging technologies in various sectors, including financial services, transport, healthcare, and public services. We submit this response to assist the developments in legislation and regulation of AI in the UK.

We would be delighted to support the work of the Committee further if helpful. Please contact Martin Cook (partner and Head of Fintech) and Tom Whittaker (Senior Associate).¹

In this response, we use 'AI' to include algorithmic decision-making (**ADM**) even if those algorithms are relatively simple. This is because use by private or public bodies of ADM can raise similar issues and risks as use of AI systems and there are parallels to be drawn.

1 HOW EFFECTIVE IS CURRENT GOVERNANCE OF AI IN THE UK?

1.1 There have been few public examples of AI systems (or ADM) causing loss or harm or otherwise not working as expected in the UK. Examples include the Judicial Review of Department for Education's use of ADM for A-level grading in 2020.

1.2 However, that does not necessarily mean that governance of AI in the UK has been effective. We may not know and may not have proxies for answering this question: it may be by luck that risks did not materialise, or because of a lack of transparency, for example, that an AI system was used, that loss has occurred, and/or that an AI system caused that loss in whole or part.

1.3 We can make the following observations:

- (a) existing regulation and guidance is fragmented and at varying stages of maturity meaning that industry (and advisers) navigate AI risks and regulations with some uncertainty;
- (b) regulators have produced useful guidance on how specific regulations may apply to AI systems. However, the breadth, detail and volume of such guidance differs depending on regulator and may take a sector- or issue-specific approach. Further, there is a risk that AI systems are not seen holistically and instead just seen as an isolated issue depending on which regulator the stakeholder is most familiar, e.g. viewing AI systems as a 'data issue' or through a financial regulation lens;
- (c) legislation and regulation were not designed for AI as a technology or for the evolving AI use cases;

¹ Martin.Cook@burges-salmon.com; Tom.Whittaker@burges-salmon.com

- (d) the common law has been flexible to applying existing legal frameworks to emerging technologies. For example, there is now established case law recognising that holders of cryptoassets may exercise and enforce property rights.² The Law Commission's report on Smart Contracts recognises this.³ However, case law is by its nature largely responsive to disputes as they arise and relatively few cases result in judgment which develop the common law. We look forward to the Law Commission's recommendations regarding digital assets, and its other work on emerging technologies; and
- (e) we note the work of the Digital Regulation Co-operation Forum and of individual regulators on whether and to what extent existing regulatory frameworks require amending.

2 WHAT ARE THE CURRENT STRENGTHS AND WEAKNESSES OF CURRENT ARRANGEMENTS, INCLUDING FOR RESEARCH?

2.1 Strengths include:

- (a) that businesses take reassurance from existing and known regulators apply existing and known regulations. Levels of venture capital investment into the UK, relative to other jurisdictions, indicates that industry has a good deal of confidence in the current regulatory landscape⁴;
- (b) the high level of engagement by certain regulators with the innovation agenda (including regulatory and digital sandboxes at the FCA and ICO plus 'policy sprints' and 'tech sprints') giving the positive message that regulators want to engage with emerging technologies in a way that embraces innovation whilst managing risk, and give participants a chance to do innovate in a risk-managed way; and
- (c) the role of bodies such as the Alan Turing Institute and Ada Lovelace Institute which bring stakeholders together and publish useful resources, including notably the AI Standards Hub.

2.2 The primary weakness is the potential for gaps in regulation and legislation, and inconsistencies between differing regulations or the application of regulation both within the UK and with international jurisdictions. Without a holistic review – either across sectors or for a specific sector – it is difficult to properly understand the scope and extent of those gaps. However, such a review would require regular update given the changing technology and use cases of AI.

² For example, *AA v Persons Unknown* [2019] EWHC 3556 (Comm)

³ <https://www.lawcom.gov.uk/project/smart-contracts/>

⁴ See OECD data: <https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data>

3 WHAT MEASURES COULD MAKE THE USE OF AI MORE TRANSPARENT AND EXPLAINABLE TO THE PUBLIC?

3.1 Government and regulators should consider:

- (a) to what extent it is the *public*, as opposed to any other AI stakeholder or legal person which may be harmed by the use of an AI system, who require transparency and explainability;
- (b) exactly what is meant by *transparency* and *explainability*, especially in the context for each stakeholder; and
- (c) what the objectives are for providing transparency and explainability – for example, building trustworthiness in specific AI systems or AI systems more generally and/or to allow for scrutiny and potential challenges to the use of those AI systems.

3.2 In order to provide transparency and explainability to the public, we expect that government and regulators will consider the use of:

- (a) independent, expert, cross-sector groups to consider what is meant by *transparency* and *explainability* for the public, and to what extent specific groups or contexts affect those meanings;
- (b) transparency notices for specific use cases and requirements for specific information to be included and in a specified format. Consideration should be given to lessons learned from use of data protection notices such as cookies notices in improving public understanding of when and how their data is used;
- (c) transparency registers for specific sectors or use cases; and
- (d) publication of impact assessment statements and policies. Again, lessons may be learned from data protection regulation around the effectiveness (or otherwise) of data privacy notices.

4 HOW SHOULD DECISIONS INVOLVING AI BE REVIEWED AND SCRUTINISED IN BOTH PUBLIC AND PRIVATE SECTORS?

4.1 The method for scrutiny will depend on the context including: the nature of the AI technology; the use-case(s); the stakeholders involved, including whether or not they are in the private or public sector; the foreseeable mis-uses of the AI system; any type and scale of actual or potential harm caused; and which individual(s) or group(s) have or may have been harmed.

4.2 However, we expect that there are overarching principles which apply, including that decisions should be scrutinised in a way which recognises:

- (a) the legitimate needs of different stakeholders, including:
 - (i) their exposure to the risk of harm;
 - (ii) their roles and responsibilities regarding the relevant AI system; and
 - (iii) protecting of specific types of information, including confidential information and personal data;
- (b) the need to identify those who risk causing harm or undermining trustworthiness;
- (c) the need and potential consequences of such scrutiny (because this will inform the speed and process with which scrutiny should be applied);
- (d) the need for consistency with applicable regulations and legislations, and recognises any potential gaps or uncertainties which affected the AI system during its lifecycle up to the point of harm being caused; and
- (e) the potential for any consequences to set a precedent, both in the UK and in other jurisdictions.

4.3 We expect that government and regulators will want to consider lessons learned from implementing data protection and freedom of information regulation and legislation, as well as efforts by other jurisdictions to scrutinise AI in both public and private sectors.

5 ARE CURRENT OPTIONS FOR CHALLENGING THE USE OF AI ADEQUATE AND, IF NOT, HOW CAN THEY BE IMPROVED?

5.1 In terms of issues with existing regulations:

- (a) *Placing on the market* – the focus on ensuring compliance at the point at which a product is placed on the market, derived from product liability laws, may not be appropriate where the AI system is dynamic and will change after entering the market;
- (b) *Liability* – the potential for lack of transparency and explainability of AI systems, and the various stakeholders involved in the AI lifecycle, impacts the ability to understand reasons for an error or malfunction and to identify who is liable for what. It will be important to make clear where regulatory responsibility lies particularly in the context of outsourced services where oversight over the third party service provider's systems and controls may be more difficult to establish,

particularly if that third party service provider is not subject to the same regulatory framework as the customer; and

- (c) *Types of harm* – the variety of uses and end users of AI systems risks causing various types of loss: economic; goodwill; physical; psychological; fundamental rights; market stability and integrity. The harm caused, and the loss suffered, may be in the virtual world as much as it is in the real world. It is unclear whether existing regulations appropriately address the various types of loss that may occur.

5.2 In terms of bringing and proceeding with challenges on the use of AI, we expect potential claimants may face issues including:

- (a) *Standing* – whether or not anyone who wishes to challenge a claim has standing to do so;
- (b) *Evidence* – there may be an information asymmetry between parties and potential claimants may have insufficient evidence to effectively make decisions about how to proceed;
- (c) *Causation* – partly arising as a result of issues with evidence, potential claimants may struggle to identify which AI stakeholder/s to pursue a legal action against and to meet any burden of proof; and
- (d) *Resources* – there may be an asymmetry in resources – financial and technical – which limits a potential claimant’s ability to bring or proceed with a claim.

5.3 One issue regulators, the courts and (potentially) legislators will need to address is how to scrutinise ‘black box’ AI systems. Regulators will need to consider whether there are circumstances in which AI does not need to be ‘explainable’. There is a trade-off between explainability and performance; the greater the performance, the more difficult it is to explain how the AI produced its output. However, regulators may need a different approach where explainability is limited or non-existent. Where that is the case, regulators may not be in a position to understand how the AI produced its output. Consequently, regulators will be left with examining the inputs and outputs only. The outputs may not appear to fall within ‘reasonable’ parameters. But the nature of AI is that it will identify unexpected patterns to produce more accurate outputs. There is, of course, a risk of fault or bias within the AI. But it remains possible that the AI correctly produces an output which appears unreasonable and for which no explanation can be given.

6 HOW SHOULD THE USE OF AI BE REGULATED, AND WHICH BODY OR BODIES SHOULD PROVIDE REGULATORY OVERSIGHT?

6.1 Absence of regulation and guidance is not an option. A vacuum of guidance results in uncertainty over when and whether regulators or legislators may take action. Regulation in some form is useful: AI brings benefits for which regulations can support; AI brings risks which regulations should address.

6.2 We are agnostic as to whether there is a single regulator or multiple regulators. There are pros and cons of the different approaches. An obvious pro of a multi-regulator approach is that there will be a high level of contextual understanding and industry specificity in the creation of guidance and in the application of supervisory and oversight functions; an obvious con is the risk of diverging approaches, standards and views (which may impact on trust, create unfairness, confusion and inefficiency – not least for those AI manufacturers and users who operate across different industry segments).

6.3 However, we do consider that there is a need for:

- (a) greater co-ordination, with clear governance structures, between regulators and non-statutory bodies to ensure a coherent approach to regulation, guidance and enforcement;
- (b) government guidance to be produced promptly and reviewed regularly as to how the cross-sectoral principles apply in practice;
- (c) clarity from government as to the types of 'high-risk' AI systems that it intends regulators to address so that it is clear to all stakeholders – including industry – which AI systems are, and are not, likely to be subject to future regulatory intervention;
- (d) clarity from government and regulators as to how different types of liability will be apportioned between the various stakeholders of an AI system (for example, between end users, intermediaries and service providers) and to what extent those liabilities change due to the dynamic nature of an AI system's lifecycle;
- (e) a clear, robust and consistent methodology for monitoring individual regulators, and the overall regulatory and legislative system, for pro-actively managing the specific risks posed by AI systems;
- (f) consistency of a definition of 'AI system' and what constitutes a reportable incident, in particular whether it involves AI as the main or a contributory causal factor, and not purely part of the factual matrix. We say this because, while we recognise the benefit of flexibility to adapt to sector and market requirements, it is also important for consistency across the market as a whole – not least in

order to provide commonality for service providers offering AI systems into multiple sectors and to assist on matters of liability and insurability.

7 TO WHAT EXTENT IS THE LEGAL FRAMEWORK FOR THE USE OF AI, ESPECIALLY IN MAKING DECISIONS, FIT FOR PURPOSE?

7.1 A holistic review of this is required but we make the following observations:

- (a) there are well established and understood legal frameworks for decision-making by different public bodies depending on the context in which they operate;
- (b) the common law is capable of adapting to emerging technologies and has a long track record of doing so in both private and public law litigation;
- (c) the court system and judges also have an established track record in adapting to emerging technologies and novel factual issues;
- (d) however, as noted above, legal frameworks were not developed with AI in mind, and development of the common law is reactive; and
- (e) we expect that there are some areas which will require specific statutory intervention. We note that the Law Commission is considering potential new laws further to its report on Smart Contracts. We also note the Law Commission's public announcement about its 14th programme of law reform questioned whether the following should be included: *'Should a legal framework be developed to support the increased automation of public decision-making?'*

7.2 We expect some legislative reforms are required to address the issues we identified in paragraph 5.3 regarding black boxes and our response to question 4.

8 IS MORE LEGISLATION OR BETTER GUIDANCE REQUIRED?

8.1 Legislation is welcomed where there are clear gaps, uncertainties or contradictions.

8.2 However, whether or not legislation is required should be considered from different stakeholder viewpoints and will depend on the risks, sector and use cases. It should also be recognised that legislation may introduce uncertainty, for example through lack of clarity or inconsistencies with other legislation.

8.3 Further legislation will occur and needs to be considered within the holistic legislative and regulatory framework; for example:

- (a) the Data Protection and Digital Information Bill proposes amendments to article 22 of the UK GDPR, in summary, when and how a data subject is subject to automated decision-making⁵; and

- (b) there are discussions about and proposals for legislative reform in specific sectors. For example, the Law Commission raising the prospect of a legislative framework for automated decision-making in the public sector⁶, and the All Party Parliamentary Group on the Future of Work] has proposed statutory rights for employees to obtain a “*full explanation of the purpose, outcomes and significant impacts of algorithmic systems in the workplace, which would include access for workers to relevant AIAs [Algorithmic Impact Assessments] and a means of redress*”.⁷

8.4 This is also because those wishing to procure, develop or deploy AI systems may look to legislation and case law for instruction or guidance, but there is limited legislation or case law specific to AI:

- (a) the Law Commission’s reports into Smart Contracts⁸ and, separately, Digital Assets⁹, and its open consultation into DAOs¹⁰, are commendable. The publications provide useful guidance as to how current laws accommodate developing technologies, where there may be novel issues, and what, if any, legal reform may be required; and
- (b) case law in England & Wales specific to AI issues is limited. Some cases are settled before a judgment is made, therefore losing the benefit of the court’s views on a potentially novel topic relevant to AI.¹¹ Case law in other jurisdictions is also limited, and where it does exist it is instructive but not determinative for how the laws would apply in England & Wales.¹²

9 WHAT LESSONS, IF ANY, CAN THE UK LEARN FROM OTHER COUNTRIES ON AI GOVERNANCE?

9.1 The UK should look to lessons from regulators and legislators in other jurisdictions. The following are useful:

- (a) The EU’s process for scoping, developing and proposing the EU AI Act, AI Liability Directive and updated Product Liability Directive is notable, in particular, the use of early engagement, stakeholder engagement, and expert groups.

⁵ For example, see the House of Commons Research Briefing on the Data Protection and Digital Information Bill (31 August 2022) <https://researchbriefings.files.parliament.uk/documents/CBP-9606/CBP-9606.pdf>

⁶ <https://www.lawcom.gov.uk/14th-programme-kite-flying-document/#AutomatedDecisionMaking>

⁷ <https://www.futureworkappg.org.uk/news/zownl0mx4t4n6smrk4dmzor0oz4djg>

⁸ <https://www.lawcom.gov.uk/project/smart-contracts/>

⁹ <https://www.lawcom.gov.uk/project/digital-assets/>

¹⁰ <https://www.lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/>

¹¹ Tyndaris, Sam v MMWVWM Ltd. Case No: CL-2018-000298

¹² B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(l) 03 <https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/b2c2-ltd-v-quoine-pte-ltd.pdf>

- (b) It is also notable how the EU proposes to use different regulations to enhance others – i.e. they are viewed and intended to work holistically – for example:
- (i) the proposed Product Liability Directive providing a compensation mechanism which the AI Act does not for those who suffer loss from AI systems;
 - (ii) the AI Liability Directive which addresses issues concerning burden of proof and disclosure where AI causes harm in response to breaches of the AI Act, thereby increasing the incentives to comply with the AI Act;
 - (iii) ensuring through drafting and stakeholder engagement that the EU AI Act does not overlap with other EU directives which seek to address similar harms, for example, financial services and medical device regulations.
- (c) Canada's Directive on Automated Decision-Making which to any system, tool, or statistical models used to recommend or make an administrative decision by the Government of Canada (with exceptions for some offices) to a member of the public - sets out transparency requirements. For example, the Government of Canada retains the right to access and test the automated decision system, including all released versions of proprietary software components, in case it is necessary for a specific audit, investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure. Source code owned by the Government of Canada may be released, subject to limited exceptions.

(November 2022)