23 September 2022

CIPL's Response to UK Department for Digital, Culture, Media and Sport (DCMS) Policy Paper on Establishing a Pro-innovation Approach to Regulating AI

I. Introduction

As an increasing number of jurisdictions consider regulatory regimes for Artificial Intelligence (AI), the United Kingdom has a unique opportunity to put forward its own vision and approach to regulating AI and demonstrate leadership on difficult and universal AI issues that different countries are thinking about from a legal and policy perspective. The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to provide input to the UK Department for Digital, Culture, Media and Sport (DCMS) on its proposed approach to regulating AI[2]. CIPL commends DCMS for engaging in a multistakeholder consultation ahead of releasing a detailed white paper setting out its approach. The UK could potentially be the first jurisdiction to create a regulatory framework for AI and it is critical that it thinks carefully about all of the relevant issues to ensure that the UK can continue to play a leading role in AI innovation globally and set a strong example for other countries considering AI regulation. In this regard, CIPL welcomes DCMS' pro-innovation approach to regulating AI.

In responding to the specific consultation questions put forward by DCMS, CIPL wishes to highlight several issues for DCMS' consideration to augment its proposed approach and ensure a future-proof, robust and realistic approach to regulating the AI ecosystem.

II. Response to Consultation Questions

Question 1: What are the most important challenges with our existing approach to regulating AI? Do you have views on the most important gaps, overlaps or contradictions?

In the consultation paper, DCMS identifies many key challenges to the UK's existing approach to regulating AI. These include (1) a lack of clarity by organizations on the application of existing legal frameworks and laws to AI, as well as on the role of different regulatory bodies in overseeing AI; (2) the risk of potentially overlapping legal requirements and regulatory roles; (3) inconsistent regulatory powers in different sectors that have an interest in overseeing AI; and (4) the fact that UK legislation has not been developed with AI in mind which has created gaps that need to be addressed. CIPL agrees with these findings and further emphasizes the need to address these core issues to ensure the success of any UK AI regime. In particular, with respect to the need for clarity on the application of existing legal frameworks and laws to

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Establishing a pro-innovation approach to regulating AI, UK DCMS, 20 July 2022, available at https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement.

AI, it would be particularly helpful if DCMS provides a comprehensive overview and analysis of the existing legal patchwork in its upcoming detailed white paper on the UK's AI regulatory regime.

Aspects of AI are already regulated under UK data protection law.[3] CIPL wishes to call DCMS' attention to the following challenges as it works towards a framework for regulating AI:

1. *Current approach to regulating automated decision-making (ADM)*

Article 22 of the UK GDPR provides that an individual has 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."[4] The former Article 29 Working Party (now the European Data Protection Board) has provided Guidelines on Automated Decision-Making[5] that interpret Article 22 as a direct prohibition on such ADM absent the existence of one of three exceptions provided by Article 22(2) (i.e., explicit consent, necessity of processing to enter or perform a contract, or compliance with a legal obligation). Globally, Article 22 has created a trend of uncertainty among organisations, as well as data privacy regulators, which are still exploring what constitutes an impactful automated decision for purposes of Article 22. In the UK, the Information Commissioner's Office (ICO) has previously noted that it is very difficult to compile a list of examples that would be thorough enough to be informative. They suggest an alternative way to think about such impacts—by asking relevant questions in a specific context. The ICO noted that certain factors may assist in this determination, such as the psychological effects of the decision and whether an individual knows that his or her behaviour is being monitored.

CIPL believes that a more appropriate approach to regulating ADM should focus on ensuring appropriate rights of review of highly impactful decisions that an individual believes were made erroneously. The Dubai International Financial Center and Brazil have adopted such an approach under their data protection laws.[6] Of course, to effectively enable such an approach, the UK should consider defining what constitutes a highly impactful decision. CIPL has collected numerous examples of what might constitute such decisions (see Appendix 1).

2. *Use of sensitive personal data to prevent and detect bias in algorithms*

Another issue associated with the current approach to regulating AI is the ability for organizations to process sensitive forms of personal information (e.g., data on race, ethnicity, gender, etc.) to prevent and detect bias in algorithms. Denying access to, or preventing retention of, such data will only make it harder to detect and remedy bias while also denying all segments of society the full potential of AI's benefits. Many data privacy laws impose specific restrictions on the processing of sensitive data. For example, in the UK, organisations are prohibited from processing such data unless a special derogation set out under Article 9 of the UK GDPR or Schedule 1 of the UK Data Protection Act 2018 (UK DPA) applies. Neither the

[3] See the UK GDPR and Data Protection Act 2018.
[4] UK GDPR, Article 22.
[5] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted 3 October 2017, revised 6 February 2018, available at https://ec.europa.eu/newsroom/article29/items/612053.
[6] See Dubai Data Protection Law, DIFC Law No. 5 of 2020, Article 29(vi), 30(vii) and 38, available at https://www.difc.ae/application/files/6115/9358/6486/Data_Protection_Law_DIFC_Law_No.5_of_2020.pdf; and Brazil General Data Protection Law (LGPD), Article 20.

UK GDPR or the UK DPA currently include an appropriate avenue for organisations to process sensitive data to mitigate bias in the AI context. CIPL recommends that the UK consider the approach under the DIFC's data protection law which provides a specific carve out for such processing. Under that law, processing of sensitive data is prohibited unless the processing is "proportional and necessary to protect a Data Subject from potential bias or inaccurate decision-making, where such risk would be increased regardless of whether Special Category (i.e., sensitive) Personal Data is processed."[7]

3. *Applicability of controller and processor concepts to AI actors*

Finally, CIPL wishes to highlight that the traditional concepts of data controllers and processors under UK data protection law are challenging to transpose to different actors in the AI context. For example, it can be difficult to classify AI developers, producers, suppliers, deployers and users as controllers or processors, especially considering these parties may have different roles with respect to the same pool of personal data in the context of different processing operations (i.e., they may be a controller for some purposes and a processor for others). The UK must ensure that these concepts are interpreted in a broad manner and flexibly to reflect the dynamic data sharing and use practices in the AI ecosystem. As such, CIPL recommends the UK consider their interpretation carefully in formulating any AI regime.

Question 2: Do you agree with the context-driven approach delivered through the UK's established regulators set out in this paper? What do you see as the benefits of this approach? What are the disadvantages?

CIPL agrees with the context-driven approach proposed by DCMS. AI is constantly developing and it is imperative that the UK create a regime that can evolve with the technology and be flexible to changes in the AI ecosystem. An overly prescriptive approach runs the risk of creating a framework that will either become quickly outdated or unnecessarily inhibit innovation.

One of the disadvantages of a context-driven approach is that it may create less certainty for organizations than a prescriptive approach. The flexible nature of a context-driven approach may also be viewed as more burdensome by organizations that will need to conduct a thorough assessment of the risks involved with the development and deployment of AI applications and consider the measures and controls to be implemented to ensure the responsible use of AI. This is especially true for smaller companies. Nevertheless, CIPL believes that such assessment and consideration of controls is critical to enabling an AI regime based on accountability. To reap the benefits of AI innovation, organizations must be mindful of the risks involved and think carefully about what is required to lower or mitigate the risks.

A risk-based approach to regulating AI is central to a robust principles and outcomes-based AI regime. The focus of such an approach assesses the risk of the impact of AI technology in the context of specific uses and applications rather than the risk of the technology in the abstract. Understanding the potential impact and any risk of harms of a specific AI application on individuals enables organizations to make risk-based decisions and implement appropriate controls and mitigations to minimize the risks involved in an AI project. By focusing on impacts and risks, organizations can determine how to allocate resources and ensure appropriate attention is paid to AI applications that pose higher risks. CIPL recommends that the

[7] Dubai Data Protection Law, DIFC Law No. 5 of 2020, Article 11(K), available at https://www.difc.ae/application/files/6115/9358/6486/Data_Protection_Law_DIFC_Law_No.5_of_2020.pdf.

UK make clear that part of the risk assessment exercise inherent to the context-driven approach is an assessment of the benefits of an AI application, including benefits to society, individuals, the public sector, organizations, for research and development, etc. For example, systems using facial recognition (FRT) and biometrics must be assessed in relation to the risk they pose in a given context – FRT does not in itself pose high risk and may, in some cases, even lower the risk of harm to individuals (e.g., use of FRT for identity verification can minimize the risk of identity theft and fraud).

One way that the UK could assist organizations to be accountable in the context of AI is to encourage regulators to create templates and guidance on risk assessment and to work with organizations through AI regulatory sandboxes. In addition, the UK should consider the value of policy prototyping projects in this regard. Policy prototyping programs are collaborative pilot projects that mobilize a coalition of public and private actors. These programs are also regulatory innovation labs intended to enable the development and testing of a policy idea in the field of new and emerging technologies, including AI. The policy idea can be inspired by a law that is being discussed, a self-regulatory instrument, a code of conduct, a set of industry guidelines, etc. Policy prototyping programs are also empirical programs that provide evidence-based policy input to policymakers either to improve existing governance frameworks or to inform new ones. A successful example of policy prototyping is Meta's Open Loop project.[8] Open Loop projects have been deployed in Europe in the context of AI risk assessments and the envisioned policy approach of the proposed EU AI Act and in Singapore and Mexico on transparency and explainability. The EU project was very useful to start-ups in the AI space which valued the process of conducting an AI risk assessment along with the guidance that was prepared for them to conduct such an assessment. Engaging in this exercise helped the start-ups to develop better AI applications early in the product development process.

Question 3: Do you agree that we should establish a set of cross-sectoral principles to guide our overall approach? Do the proposed cross-sectoral principles cover the common issues and risks posed by AI technology? What, if anything, is missing?

CIPL welcomes the cross-sectoral principles put forward by DCMS. These principles touch upon important issues, including safety, functionality, transparency and explainability, fairness, legal responsibility for AI governance and redress and contestability.

CIPL recommends that the UK include a specific overarching principle on accountability to the cross-sectoral principles. Accountability is a bedrock principle upon which the UK's AI regime should be based. Accountability requires organizations to operationalize and translate principles-based rules through appropriate and demonstrable policies, procedures, controls and governance to deliver compliance. Accountability also enables the adaptation of principles-based rules to specific industries, technological applications and differing levels or risk. The UK should also consider establishing the specific elements and expected outcomes of accountability in its AI regime both for the benefit of organizations as well as regulators who may elaborate on the elements in the context of their specific sector. There are different approaches to breaking down accountability into its constituent parts. One approach that is gaining

[8] See "Introducing Open Loop, a global program bridging tech and policy innovation", available at https://ai.facebook.com/blog/introducing-open-loop-a-global-program-bridging-tech-and-policy-innovation/; and AI Impact Assessment: A Policy Prototyping Experiment, available at https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3772500_code715910.pdf?abstractid=3772500&mirid=1.

traction among organizations and regulators is the use of an accountability framework, such as the framework created by CIPL (see below).

Accountability Element	Description
Leadership and Oversight	**Establishing leadership and oversight for the responsible use of AI**, including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's AI accountability program and report to management and the board.
Risk Assessment	**Assessing and mitigating the risks** that AI applications may raise to individuals, including weighing the risk of the AI use against its benefits.
Policies and Procedures	**Establishing internal written AI policies and procedures** that operationalize legal requirements and create concrete processes and controls to be followed by the organization, reflecting the identified risks, applicable law, regulations, industry standards as well as the organization's values and goals.
Transparency	**Providing transparency to all stakeholders internally and externally** about the organization's AI practices, the rights of individuals in relation to their data and the benefits and/or potential risks of AI applications. This may also include communicating with relevant regulatory authorities, business partners and third parties about the organization's AI practices.[9]
Training and Awareness	**Providing training for employees** to ensure awareness of the organization's AI practices. This ensures AI accountability is embedded in the culture of the organization.
Monitoring and Verification	**Monitoring and verifying the implementation and effectiveness of the AI accountability program and internal compliance** with the organization's AI practices and controls through regular internal or external audits and redress plans.
Response and Enforcement	**Implementing response and enforcement procedures** to address inquiries, complaints and internal non-compliance, and to enforce against acts of non-compliance with the organization's AI accountability program.

[9] To provide effective transparency in the AI context, organizations will need to consider the specific audience involved. For instance, information about the inner workings of algorithms may be inappropriate and not useful to individuals who challenge the results of an automated decision. In contrast, in the context of a regulatory investigation, it may be necessary to provide more detailed information about how an AI system works to a regulator. In addition, organizations will need to balance the provision of transparent information with the need to ensure that intellectual property and proprietary information remain appropriately protected. As such, it can be helpful to consider the different goals of transparency in the AI context (i.e. provision of information to specific audiences to achieve understandability, traceability, explainability, articulation of benefits or individual rights and avenues for redress). By considering these factors and goals, organizations can make contextual decisions to ensure that the right level of information is provide to the specific audience involved.

Figure 1 – CIPL Accountability Framework – Universal Elements of Accountability

Question 4: Do you have any early views on how we best implement our approach? In your view, what are some of the key practical considerations? What will the regulatory system need to deliver on our approach? How can we best streamline and coordinate guidance on AI from regulators?

CIPL supports the UK's proposed approach to regulating AI that is context-driven, based on cross-sectoral principles and implemented by the UK's existing regulators. CIPL wishes to underline several considerations that DCMS should consider as it crafts a detailed white paper on the UK's AI regulatory regime.

Firstly, there is a risk that the proposed approach, if not appropriately implemented, could lead to divergent regulatory approaches, views and guidance and could create more harm than good for organizations and individuals. DCMS should specify in its upcoming white paper which regulators it envisions will play a leading oversight role for any AI framework established in the UK. In particular, it should clarify that the ICO will retain competence over AI applications involving the processing of personal data and/or impacting individuals' privacy rights. Moreover, DCMS should emphasize that regulatory cooperation and coordination will be key to preventing divergence and that regulatory hubs and cooperation forums (such as the UK Digital Regulation Cooperation Forum[10]) will be critical to ensuring consistent interpretation of AI principles, oversight and enforcement. Finally, DCMS should consider how organizations will practically engage with regulatory bodies under a new AI framework, including options to engage with a single point of contact.

[10] UK Digital Regulation Cooperation Forum, available at https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

Secondly, regulators will have an important role to play in incentivizing accountability to successfully implement its proposed approach. Regulators will need to encourage organizations to adopt the cross-sectoral principles and outline the benefits of doing so to promote their uptake. This may include highlighting that organizations who adopt the principles can engage in certain further uses of AI technology and that adoption of the principles will be considered as a mitigating factor in any enforcement action.

Thirdly, the UK's AI regime should promote the creation of modern and agile regulatory oversight tools such as regulatory sandboxes, policy prototyping projects and data review boards. These tools can be very useful to assist and shepherd organizations in adopting the principles. These tools also provide avenues for regulators to collaborate on AI issues and find common solutions to pressing issues. For example, sectoral regulators could create cross-sectoral AI sandboxes.

Fourthly, to ensure the successful implementation of the UK's proposed approach to regulating AI, DCMS and regulatory authorities must consider the impact of such an approach on industry and on AI technology. They can do so through engaging in a multistakeholder process on the building of the proposed regime and on the creation of any subsequent guidance and sectoral applications of the regime. Moreover, CIPL recommends creating special advisory boards and committees to work with regulators and organizations to collate different views and vet guidance. The UK Centre for Data Ethics and Innovation (CDEI)[11] could provide specialist knowledge and expertise in this regard and could even create an industry pool of experts or review bodies to contribute to regulatory guidance.

Finally, the UK must consider how the proposed regime will work with existing laws, including in areas of data protection, tort, commercial contracting, consumer safety, product liability, etc., and whether any of these requirements conflict with the proposed regime and how to resolve such conflicts.

Question 5: Do you anticipate any challenges for business operating across multiple jurisdictions? Do you have any early views on how our approach could help support cross-border trade and international cooperation in the most effective way?

As noted above, an increasing number of countries are considering the creation of AI regulatory regimes, notably the European Union, Brazil and China. Diverging global rules and legal frameworks for AI have the potential to create significant burdens for multinational organizations and the global AI innovation landscape. DCMS has correctly identified the need to ensure interoperability and promote the responsible development of AI in a global market. As such, CIPL supports the UK's desire to continue to play an active role in organizations such as the Global Partnership on Artificial Intelligence (GPAI) and the OECD and to serve as a pro-innovation voice in ongoing Council of Europe negotiations.

In addition to these efforts, CIPL recommends that the UK engage in bi-lateral discussions on AI with nations considering AI regulation and share knowledge and experience as the UK builds its own regime. In the context of data protection, the UK ICO should continue to engage on AI issues in fora such as the

[11] Centre for Data Ethics and Innovation, available at https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation.

Global Privacy Assembly (GPA), the Common Thread Network (CTN), the Global Privacy Enforcement Network (GPEN), etc.

Finally, CIPL recommends that UK engage in capacity building exercises with other nations on creating a legal framework for AI based on accountability, once the UK has finalized the structure of its AI regime. Such exercises serve to educate other nations on successful approaches in other countries and can provide an outlet for the UK to promote its own approach.

Question 6: Are you aware of any robust data sources to support monitoring the effectiveness of our approach, both at an individual regulator and system level?

CIPL believes that the UK can employ several mechanisms to monitor the effectiveness of its approach to regulate AI. Firstly, regulators should be entrusted with monitoring the application of the approach in their respective industries and publish their finding and analysis to provide feedback to the UK government. Regulators should analyse, in particular, any trends or patterns in complaint handling on AI issues. Such patterns can serve as a useful indicator of how effective the AI framework is. For example, if there are thousands of complaints on a specific AI issue, the UK may need to consider if the framework needs to be updated or amended in light of those complaints. Secondly, the UK should consider the role of certification bodies in the UK to monitor the effectiveness of the AI framework.

III. Conclusion

CIPL is grateful for the opportunity to provide input to DCMS on its proposed approach to regulating AI. CIPL supports the overall approach and believes that by incorporating the recommendations outlined throughout this paper, DCMS will be able to augment the proposed framework in a way that will ensure it remains future-proof and fit for the modern digital AI economy, and provides appropriate protection for individuals and society without hampering the ability of organizations to engage in AI innovation. CIPL looks forward to reviewing DCMS' upcoming and more detailed white paper on the UK approach to regulating AI as well as further opportunities to provide feedback as the UK works towards creating an AI regime for the future.

If you would like to discuss any of the comments in this paper or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

Appendix 1 - Examples of Automated Decisions Producing Legal and Similarly Significant Effects

Decisions Producing Legal Effects	• Decisions affecting the legal status of individuals • Decisions affecting accrued legal entitlements of a person • Decisions affecting legal rights of individuals • Decisions affecting public rights — e.g., liberty, citizenship, social security • Decisions affecting an individual's contractual rights • Decisions affecting a person's private rights of ownership
Decisions Producing Similarly Significant Effects *Some of these examples may also fall within the category of legal effects depending on the applicable legal regime and the specific decision in question*	• Decisions affecting an individual's eligibility and access to essential services — e.g., health, education, banking, insurance • Decisions affecting a person's admission to a country, their citizenship, residence or immigration status • Decisions affecting school and university admissions • Decisions based on educational or other test scoring – e.g., university admissions, employment aptitudes • Decision to categorise an individual in a certain tax bracket or apply tax deductions • Decision to promote or pay a bonus to an individual • Decisions affecting an individual's access to energy services and determination of tariffs
Decisions <u>Not</u> Producing Legal or Similarly Significant Effects *These automated decisions do not typically produce such effects. Instances where they might produce such effects are contextual and should be determined on a case-by-case basis.*	• Decisions ensuring network, information and asset security, and preventing cyber-attacks • Decisions to sandbox compromised devices for observation, restrict their access to or block them from a network • Decisions to block access to malicious web addresses and domains and delivery of malicious emails and file attachments • Decisions for fraud detection and prevention (e.g., anti-fraud tools that reject fraudulent transactions on the basis of a high fraud score) • Decisions of automated payment processing services to disconnect a service when customers fail to make timely payments • Decisions based on predictive HR analytics to identify potential job leavers and target them with incentives to stay • Decisions based on predictive analytics to anticipate the likelihood and nature of customer complaints and target appropriate proactive customer service • Normal and commonly accepted forms of targeted advertising • Web and device audience measurement to ensure compliance with advertising agency standards (e.g., requirements not to advertise foods high in fat, sugar and sodium when the audience consists of more than 25% of children)