The Rt Hon the Baroness Stowell of Beeston MBE
Chair of the Select Committee on
Communications and Digital
House of Lords
London
SW1A 0PW

9 October 2023

Dear Baroness Stowell

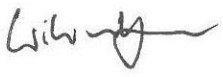
Thank you for your letter of 14 September to Sarah Cardell regarding the Committee's inquiry into large language models.

I absolutely agree that there is potential for AI to transform a wide range of services and be the catalyst for significant innovation and competitive disruption in markets. Competition and compliance with consumer law is vital to ensure people get the full benefits that FMs have to offer. That is why the CMA has put itself on the front foot with that thinking, rather than waiting for problems to emerge and only then stepping in with corrective measures. Our initial review of AI foundation models (FMs) has proposed guiding principles which aim to ensure consumer protection and healthy competition are at the heart of responsible development and use of FMs.

While I hope that our collaborative approach will help realise the maximum potential of this new technology, we are ready to intervene where necessary.

Please see attached our responses to the questions you have raised. I would be very happy to discuss further or provide additional information. I look forward to giving evidence to the Committee in November.

Yours sincerely,



Will Hayter
Senior Director, Digital Markets Unit
Competition and Markets Authority

Response to Committee questions

This response refers to the CMA's AI-related work. Although the scope of such work is not all limited to LLMs, the issues raised are often similarly applicable to LLMs.

1. How many staff do you employ specialising in AI-related governance (if any)?

1.1. The CMA does not employ any dedicated staff specialising in AI-related governance (we interpret this to mean address AI-related harms within our competition and consumer protection remit).

1.2. The CMA's general operating model involves setting up multi-disciplinary teams of policy, legal, economic and technologist staff to deliver discrete projects. At the end of such projects, staff are redeployed to other cases and projects. However, we are building more long-term expertise on AI, particularly in the CMA's Digital Markets Unit (DMU) and Data, Technology and Analytics (DaTA) teams.

1.3. For example, the CMA recently carried out an initial review of FMs (FMs initial review).[1] The aim of the review was to develop an early understanding of the market for FMs and how their use could evolve; what opportunities and risks these could bring; and what competition and consumer protection principles will best guide the development of these markets in future. Around 15-20 people contributed throughout the project, equivalent to around 10 FTE over the four months. Following the FMs initial review, we are also starting a significant programme of further engagement. We plan to speak to a wide range of people to seek views on our report and the proposed guiding principles.

1.4. In the past few years, six staff across both the DaTA team and the DMU have been involved in the following AI-related initiatives:

- Coordinating the policy work on AI across the CMA, through a CMA AI working group. The AI working group also has a horizon-scanning function.

- Cooperating in workstreams on AI-related governance in the Digital Regulation Cooperation Forum (DRCF), including:

    - **Algorithmic processing** – this workstream helps coordinate DRCF members' engagement with the Office for AI, among other projects and objectives; and

    - **Enabling innovation** – this workstream is leading the response to the recommendation of the Vallance Review to establish a Digital and AI regulatory advice service for innovators (formerly

[1] The scope of the FMs initial review is different to the scope of the Committee's inquiry on LLMs. The initial review focused on foundation models, which is defined as a machine learning model which is trained on vast amounts of data and can be adapted to a wide range of tasks and operations.

known as an 'AI sandbox').

- Engaging with Office for AI, CDEI, the Alan Turing Institute (ATI) and other stakeholders, including through responding to information requests, attending meetings and workshops to assist in the development AI regulation policy, and responding to the Government's policy proposals and white paper on AI regulation.

1.5. In addition, the DaTA team has a continuous, business-as-usual horizon-scanning function that monitors developments in emerging technologies and digital markets. It also produces internal briefings and primers on significant topics and developments. Unsurprisingly, AI-related developments (including on AI governance) have featured heavily in the work of this function in recent years, which preceded the FMs initial review. Over the last two years, the function has been staffed by between two to four colleagues.

1.6. The CMA also leverages AI-related technical expertise through its Digital Experts Panel. This panel of nine experts are appointed in an advisory capacity and bring independent insight and practical experience and support the CMA's work in digital markets and recently contributed to the CMA's initial review.[2]

2. How many data scientists (or equivalent) do you employ (if any)?

2.1. The CMA's DaTA team has nine data scientists and approved funding for five additional data scientist positions of varying grades, seniority and experience.

2.2. The CMA's data scientists provide the CMA with:

- Machine learning analysis of large datasets acquired by the CMA to support its investigations;
- Machine learning expertise to advise CMA's investigations on how companies may be using machine learning and AI; and
- Development of machine learning-based tools to improve the operational efficiency of the CMA e.g. using natural language processing techniques in evidence review to automatically extract information from text.

2.3. The data scientists are supported by:

- Three data engineers (although we have approved funding for three additional data engineer positions), and
- 20 technologists that provide broader technical research, technology policy advice and horizon-scanning.

[2] Experts appointed as UK looks to level digital playing field for consumers - GOV.UK (www.gov.uk)

3. Do you anticipate these figures changing significantly in the next three years?

3.1. The CMA is starting the next phase of its work on foundation models, as well as continuing joint work with our fellow regulators through the DRCF.

3.2. The CMA is also exploring the size and design of its DaTA team in anticipation of the new duties and responsibilities through the Digital Markets, Competition and Consumers (DMCC) Bill. It is possible that the number of data scientists may change as a result.

4. Do you expect any new regulatory issues of concern to arise within your remit in the next three years in relation to advances in large language models?

4.1. We outline below the potential issues of concern that may arise within the CMA's competition and consumer remit, as set out in our FMs initial review and our 2021 research paper on algorithmic processing.[3]

4.2. Many of these potential issues are not 'new' because they relate to concerns that the CMA is used to dealing with under our existing tools, i.e. merger control, competition law enforcement (including anti-competitive agreements and abuse of dominance), market studies and investigations, and consumer law enforcement. However, what is new is the potential scale and speed of impact of LLMs on many markets. This poses a 'new' regulatory challenge for the CMA. We discuss these further below and in **question 9**.

FMs initial review

4.3. The evidence from our initial review points towards the potential for FMs to transform a wide range of services and be the catalyst for significant innovation and competitive disruption in markets. Competition and compliance with consumer law is vital to ensure people get the full benefits that FMs have to offer.

4.4. If competition is weak, people and businesses could be harmed both immediately and over the longer term. Immediately for consumers if they are exposed to significant levels of false information, AI-enabled fraud, or fake reviews; and over the longer term if a handful of firms gain or entrench positions of market power and fail to offer the best products and services and/or charge high prices. It is essential that these outcomes do not arise.

4.5. To mitigate these risks (which are further discussed in the Annex to this response) the CMA has developed a set of proposed principles for the development and use of AI foundation models.

[3] Algorithms: How they can reduce competition and harm consumers - GOV.UK (www.gov.uk)

2021 research paper on algorithmic processing

4.6. In this paper, the CMA looked at the potential competition and consumer harms from algorithms, of which LLMs is a subset.[4]

4.7. The paper found that algorithms are an integral part of how many markets and firms operate. However, firms may also misuse them, whether intentionally or unintentionally, and can cause harms to consumers and competition, often by exacerbating or taking greater advantage of existing problems and weaknesses in markets and consumers.

4.8. These include direct harms to consumers, many of which involve personalisation. Personalisation can be harmful because it is difficult to detect either by consumers or others, targets vulnerable consumers or has unfair distributive effects.

4.9. Algorithms can also be used to exclude competitors and reduce competition. For example, a platform may use algorithms to preference its own products.

4.10. In addition, the market positions of the largest gateway platforms are substantial and appear to be durable, so unintended harms from their algorithmic systems can have large impacts on other firms that are reliant on the gateway platforms for their business.

5. Do you anticipate a requirement to conduct an audit of algorithmic processes used in large language models in the next three years? (For reference we refer to the criteria set out in a paper by the Digital Regulation Cooperation Forum on algorithmic audits: governance, empirical, and technical. Please provide an indication for each of these three types).

5.1. It is possible that in conducting a market study or investigation, carrying out work under the expected pro-competition digital markets framework, or taking enforcement action in relation to particular firms, it may be necessary to audit and understand how key systems of those firms operate (e.g. those systems that underpin the products and services or those that drive the potentially problematic conduct that are the focus of the investigation).

5.2. Similarly, where we have made a relevant finding and issued an order or directions, or where firms have offered legally binding commitments to resolve our concerns, these remedies may involve ongoing monitoring requirements. Those monitoring requirements could involve regular audit or assurance of those key systems, to ensure that firms continue to be compliant. If and where these systems include use of LLMs, these may be included in the audit.

5.3. In almost every case where audit of key systems (including any LLMs or LLM component) is required, the CMA will request information that amounts to a

[4] Algorithms are sequences of instructions to perform a computation or solve a problem. The term 'algorithm' includes simpler sets of rules as well as more advanced machine learning or artificial intelligence (AI) code.

governance audit of the relevant systems (within the meaning of the DRCF paper on algorithmic audits). We would also be prepared to carry out empirical and technical audits, as needed, and would be well-equipped to do so. For further discussion on our LLM auditing capabilities, see **question 6** below.

6. Notwithstanding your answer to question 5, do you believe your organisation is well positioned to conduct audits of large language models at the (a) development and (b) deployment stage, to ensure compliance with your existing duties and the expectations in the Government's white paper?

6.1. To assess questions relating to the White Paper's principles, e.g. transparency and accountability, insofar as they intersect with the CMA's competition and consumer remit, it is likely to be important to review the policies, disclosures, terms and conditions etc associated with the deployment of LLMs, rather than just the models themselves. This review might include for example working with firms that deploy LLMs to assess compliance with consumer law, or to assess whether LLMs are being used in a way that is anti-competitive, e.g. to carry out anti-competitive self-preferencing.

6.2. The CMA may need to carry out audits of LLMs under the new digital markets regime, which includes additional tools to observe, and where appropriate, conduct tests on designated firms' systems. However, these new investigatory tools will not extend to the CMA's competition and consumer functions. See further discussion in question 9 below.

6.3. Even with the additional investigatory tools under the DMCC Bill, the CMA's role would likely focus on reviewing Strategic Market Status (SMS) firms'[5] own plans for reviewing the behaviour of their LLMs (including through a governance, empirical and/or technical audit) rather than the CMA auditing the models itself.

6.4. Looking at AI systems more widely than LLMs, the CMA is well positioned to audit algorithms and assess their potential harms on consumers and negative impact on competition. The CMA published a research paper on this subject in 2021[6], describing these potential harms and setting out a range of approaches to measure them. This remains an active area of interest for the CMA, both in terms of general research and in the context of specific cases and investigations.

7. Please could you provide an estimate of how many comparable audits

---

[5] The CMA will have powers to designate the biggest digital with Strategic Market Status (SMS) and, for those designated firms: (1) set ex ante Conduct Requirements i.e. upfront rules on how firms are expected to behave (2) enforce ex post Pro-Competition Interventions to remedy competition problems; and (3) require the firms to report merger transactions to the CMA prior to completion.

[6] https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers#techniques-to-investigate-these-harms

you have undertaken in the last five years?

7.1. The CMA has not conducted any audits of LLMs within the last five years.

7.2. We completed around ten investigations of large sociotechnical systems – comparable to governance and empirical audits. Some of these were public investigations and a minority of them were internal only, i.e. to develop the CMA's own understanding but not leading to any formal action.

8. In your view, what are your main powers and duties most applicable to delivering on the five principles set out in the white paper?

8.1. As set out in the CMA's response to the White Paper[7], the CMA's powers that are most applicable to delivering the White Paper's five principles are:

- **Consumer protection** – for example, under Principle 1 (Safety, security and robustness), we have an ongoing enforcement case against Amazon and Google in relation to potential breaches of consumer protection law. These cases are based on our concerns that Amazon and Google have not been doing enough to tackle fake reviews on their websites. This includes whether their relevant AI detection systems are sufficiently robust to circumvention by bad actors.
- **Competition** – for example, Principle 2 (Appropriate transparency and explainability) is likely to be important for our competition objective. Transparency can be important where firms with market power operate AI systems that have substantial influence over other firms' access to customers, such as whether they are recommended or ranked prominently.
- **New digital markets regime under the DMCC Bill** – under Principle 4 (Accountability and governance), the CMA may be able to hold firms accountable directly through the new proposed ex ante functions in the DMCC Bill. For example, if a firm is designated as having SMS and the relevant algorithmic activity is within the scope of its SMS designation, it would fall within the remit of the digital markets regime.

9. Are there any areas where you anticipate your existing powers and duties will fall short of what is needed to deliver against the expectations in the white paper?

<u>AI interrogation tools</u>

9.1. To address both current and emerging AI risks, it is critical for the CMA to be able to interrogate AI in its working context. This would allow the CMA to effectively implement the five principles[8] in the White Paper within its competition and consumer protection remit, including to (1) detect breaches,

---

[7] See paragraph 6(a), 11-17 of the CMA's response at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1160272/AI_regulation_-_a_pro-innovation_approach.pdf

[8] Principles are safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.

and where necessary, to gather evidence to bring an infringement case; (2) design remedies in a way that is more tailored, proportionate and effective; and (3) carry out ongoing monitoring of remedies to ensure they sufficiently address the harm.

9.2. However, the CMA across its current tools is generally limited in its ability to interrogate AI in its working context because it is unable to conduct tests on a firm's algorithms. For example, the CMA currently lacks the power to require a business to input specific prompts to the business' AI algorithm and to provide the CMA with the outputs. This could be a problem, for example, where anti-competitive activities are carried out using AI systems.

9.3. As part of its investigatory tools for the digital markets regime in the DMCC Bill, the CMA will be able to observe, and where appropriate, conduct tests on designated firms' systems. One potential use of these tools is to understand the effects of a firm's algorithms on competition and consumers. This is a welcome step and will be essential to ensuring that the CMA can effectively address the risks associated with such systems.

9.4. However, these new investigatory tools will not extend to the CMA's competition and consumer enforcement functions. This could hamper the CMA's ability to enforce competition and consumer law in AI-related activities, for the reasons discussed above.

Practical challenges to investigating and addressing AI risks

9.5. Even with the enhanced investigatory tools outlined above, the CMA faces some practical challenges in effectively investigating and addressing AI risks.

9.6. First, it can be difficult to get sufficient information from firms on their AI systems, such as sufficiently detailed description of their training data. It can also be challenging to get API access to AI systems, especially where the API[9] has been developed solely for internal purposes.

9.7. Second, the CMA faces an ongoing challenge to attract and retain people with the necessary skills in AI, machine learning and engineering, especially as we are competing with the private sector for this sought-after expertise.

10. How confident are you that there are sufficient co-ordination structures, independent of Government, between regulators outside the Digital Regulation Cooperation Forum in relation to regulating large language models?

(If applicable): please provide examples of established structures that are working well.

10.1. Current co-ordination structures between regulators outside of DRCF include: (1) the Regulators and AI Working Group, which meets quarterly and

[9] An API (application programming interface) is a method for 2 or more computer software to communicate.

is run by the ICO and 2) ATI's AI Standards Forum for UK Regulators.

10.2. The approach and resources devoted to AI and LLMs by regulators will naturally vary according to their regulatory focus, which will also affect their participation in co-operation fora and therefore the effectiveness of those structures.

Annex: Summary of risks to competition and consumer protection in the FMs initial review

1. In our initial review, we looked at (1) competition in the development of FMs (2) the impact of FMs on competition in other markets and (3) consumer protection.

2. The development and use of AI is in the early stages. It is still unclear how AI will evolve and what its long-term impact will be on society. However, in addition to a number of potential benefits, there are also risks associated with AI and it is important to start thinking about how to manage these risks.

3. We identified a number of uncertainties that could, if they manifest, lead to risks to competition and consumers. In summary:

    - **Development of FMs.** A concerning market outcome that could weaken competition in the development of FMs may emerge if access to inputs is restricted so only a handful of firms can create and maintain the leading models. As a result, those remaining firms would develop positions of strength which could give them the ability and incentive to provide models on a closed-source basis only and to impose unfair prices and terms. Any resulting reduction in competition may result in reduced incentives to innovate and this could reduce the scope for competitive innovation by a range of different firms, which may have a negative effect on economic growth and productivity.

    - **Impact of FMs in other markets**. There would be a risk to competition in downstream markets that use FMs in products/services (downstream FM services) if there is a lack of innovative FM deployment options that downstream firms can easily switch and multi-home between. Other risks to downstream competition include: (1) significant data feedback effects that may tip the downstream market towards concentration (2) consumers' inability to meaningfully choose between FM services or switch away from downstream ecosystems and (3) vertical integration and partnerships that harm competition or restrict businesses' choices. There could be particular risks to competition if firms unfairly gain or entrench their market positions through leveraging their positions in adjacent downstream markets or in the upstream development of FMs, including as providers of key inputs to FMs.

    - **Consumer protection.** Consumers need accurate and reliable information about the products and services they are using to make informed and effective decisions. A more concerning outcome for consumers could be more likely where (1) appropriate information about the FM is not presented clearly to consumers (2) consumers

have limited understanding of the limitations of FM applications, including hallucinations (3) FM applications are not designed to consider consumers' interests (4) consumers are unable to compare and switch between FM applications due to lack of external quality metrics and (5) lack of consumer redress.

4. We proposed seven competition and consumer protection principles, to help steer the market towards more positive outcomes. These are shown in the figure below. We have started a programme of collaborative engagement with a wide range of stakeholders, including consumer groups, leading FM developers, possible innovators, challengers and new entrants, businesses that use FMs, academics, governments and fellow regulators. We are seeking feedback on the proposed the principles and how they can be delivered. We hope that our collaborative approach will help realise the maximum potential of this new technology, but we are ready to intervene where necessary.