Algorithms: how they can reduce competition and harm consumers

Summary of responses to the consultation

May 2021
CMA141con

1. Contents

2. Introduction

2.1 The Competition and Markets Authority (CMA) is the UK's primary competition and consumer authority. It works to promote competition for the benefit of consumers, both within and outside the UK, to make markets work well for consumers, businesses and the economy.

2.2 The CMA published a research paper on the potential impact of the use of algorithms from a competition and consumer perspective. The paper and ongoing internal and external engagement will be used to inform the work of the CMA's Analysing Algorithms programme.

2.3 The CMA ran a consultation from 19 January 2021 to 16 March 2021 regarding the research paper. This document summarises the responses received. The consultation document and respondents' full responses are available on the consultation page.

3. Issues raised during the consultation

3.1 The CMA's consultation sought views on the following questions:

(a) Are the potential harms set out in the review paper the rights ones to focus on for our algorithms programme? Are there others that we have not covered that deserve attention?

(b) Do you agree with how we have described each harm? Are there other examples that demonstrate them in addition to the examples we have included?

(c) How likely and impactful are the identified harms now, and how might they evolve in the next few years?

(d) Are there specific examples that we should investigate further to consider whether they are particularly harmful and potentially breaching consumer or competition law?

(e) Are there any examples of techniques that we should be aware of or that we should consider beyond those that we've outlined?

(f) Are there other examples where competition or consumer agencies have interrogated algorithms that we have not included?

(g) Is the role of regulators in addressing the harms we set out in the paper feasible, effective and proportionate?

(h) Are there other ideas or approaches that we should consider as part of our role?

3.2 The CMA received 35 responses to the consultation. The respondents are listed in Appendix A, and non-confidential versions of all submissions are available on the consultation page.

3.3 Most respondents agreed that the CMA had identified the right harms to focus on. Respondents noted several nuances to the harms identified, where harms were missing, and highlighted the need for legal analysis, empirical evidence, and a proportionate approach for any investigation into the harms outlined. A summary of respondents' further thoughts and reflections is provided below.

Missing harms that deserve attention

3.4 In this section, we summarise responses related to our question: Are the potential harms set out in the review paper the rights ones to focus on for our algorithms programme? Are there others that we have not covered that deserve attention?

Consumer harms from firms' use of data

3.5 Several respondents were concerned about the increasing asymmetry of information and power between companies that collect data and the consumers from whom they collect the data. They noted that this also has implications for consumer privacy. One solution proposed was the use of personal online data stores, where consumers have control over their data.

3.6 Consumers could also face discrimination through the use of their data beyond protected characteristics. For example, discriminatory practices could be based on socio-economic categories, locking in pre-existing disparities. Some respondents noted that some companies were using proxies for protected characteristics such as gender and race to determine insurance premiums. It was suggested that in cases where market access was denied based on this type of harm, an appeal process should be implemented.

Economic harms arising from the sharing of consumer data

3.7 The control and use of data as a form of market dominance was noted by several respondents. This could include, for example, companies selectively sharing data with certain partners through mergers and cooperation agreements, to the detriment of competitors. They noted that this type of privileged access to data could be used to implement targeted pricing, ranking or self-preferencing practices.

3.8 Some respondents also proposed that the role of 'single sign on' approaches be considered, for example where the exchange of data between apparently unrelated sites could compound the identified harms in the paper and reinforce oligopolistic practices in a way that would not be possible without data and algorithmic interdependencies.

3.9 Respondents also noted that issues around algorithms used to manage business-to-business competition in supply chains were missing from the paper.

Harms from technologies associated with algorithms

3.10 Some respondents noted that harms could arise from underlying technologies or technical infrastructure underpinning consumer-facing services. For example, if infrastructure markets such as cloud computing were highly concentrated, this could limit the choice of services for consumers. In addition, where access to infrastructure is limited, this could limit consumers’ access to certain markets and result in digital exclusion.

3.11 Respondents also highlighted that off-the-shelf algorithmic systems, such as AI-as-a-Service, underpin many consumer-facing platforms, services and applications, and their use would grow in the future. They were concerned that problems these systems can exhibit, such as bias, would affect all customers of firms using them, and therefore make the issues much more widespread.

3.12 Another technology cited by respondents as growing in importance was the Internet of Things (IoT), which would bring about a shift in algorithmic harms taking place largely online to physical environments. It was suggested that this would require a more anticipatory approach from regulators regarding business-to-consumer and consumer-to-consumer e-commerce based on IoT.

Harms to citizens

3.13 Some respondents noted that algorithms could harm people as citizens. For example, democracy could be negatively impacted by publisher content being downranked unexpectedly, leading citizens as consumers of news to have inconsistent and unpredictable access to information. Examples such as this could lead to the greater societal harm of a lack of trust in algorithms.

3.14 Others noted that young peoples’ wellbeing could be negatively affected by algorithms, whether through erosion of privacy, safety and trust, or excessive screen time and related social isolation problems. Of particular concern was targeting of online advertising and social media based on fine-grained behavioural and demographic data about users, which could create addictive personalised content.

Descriptions of harms in the review paper

3.15 In this section, we summarise responses related to our question: Do you agree with how we have described each harm, and are there other examples that demonstrate them in addition to the examples we have included?

Benefits of algorithms

3.16 Several respondents noted that there were many benefits of algorithms, which could have been highlighted more in the paper. They noted that when considering harms, it was important to balance the benefits against the harms when considering any intervention.

3.17 Some respondents considered that there were also risks in not using algorithms in certain contexts, for example where they can be used to mitigate existing harms.

Empirical evidence for each harm

3.18 Many respondents commented on the need for empirical evidence for each harm. This could help, for example, to quantify the impact and frequency of harms and benefits of algorithms.

3.19 Some respondents cautioned that establishing a causal link between a harm and an algorithm or algorithmic system would be challenging, and that it would be more likely that regulators would detect correlations. They noted that it would be important to understand the context in which potential harms are identified and remedies applied.

Legal analysis required

3.20 Several respondents noted the need for legal analysis of each harm identified in the paper, as well as guidance on how the harms would be assessed and enforced. In addition, clarity was needed on which legal framework would apply to each harm, whether competition law, consumer law, or the proposed *ex ante* regime of the Digital Markets Unit.

Personalisation and personalised pricing

3.21 Respondents noted that some granularity was required in considering personalised pricing, and that it would be useful to distinguish between good and bad practices. For example, some respondents noted that personalised prices for individuals would reduce consumer welfare by offering the individual the maximum price that individual is willing to pay, thereby leaving that individual with no consumer surplus. However, quantity discounts (e.g. “12 for the price of 10”) could enhance consumer welfare by resulting in fewer numbers of larger sales (and thereby increasing efficiency) and encouraging more consumption and production and increasing economies of scale, bringing down the price of each item for all consumers of that product. In addition, respondents noted that using proxies such as ‘student’ or ‘Over 65’ to identify different groups' willingness to pay could increase consumer welfare, also by encouraging the production of additional units of a product, reaping economies of scale, and leading to potential reductions in price. In addition, personalised pricing in areas such as financial services could incentivise good customer behaviours, such as better financial or risk management.

3.22 Other respondents highlighted the negative effects of personalisation, particularly on the marketplace of ideas. They noted that if consumers do not know what is available to other people due to a lack of transparency, they are not able to freely choose the information they see.

3.23 Respondents also reflected on the discussion in the research paper of personalisation as a problem particularly for consumers with vulnerabilities or protected characteristics. They suggested going beyond vulnerabilities to consider 'susceptibilities' that could be just as detrimental to consumers, such as personalisation generating and exploiting insecurities, weaknesses and biases.

3.24 There was a comment on the personalised pricing example regarding Uber. In particular, Uber noted that they do not take into account any rider-specific or any device-specific (for example payment method or low battery) information for the purpose of pricing.

Self-preferencing

3.25 Some respondents commented that the concept of self-preferencing could be expanded to include differentiated treatment, for example in platform-to-business relations. Anti-competitive effects could be created where platforms treat non-affiliated businesses differently based on, for example, fees paid to the platform.

Ranking algorithms and recommender systems

3.26 Respondents noted a lack of transparency in how search result rankings are determined. This resulted in a distortion of consumer choice and impacted on innovation and investment.

3.27 Respondents also noted that in retail search result rankings, paid advertisements should be labelled as distinct from organic search, while trademarked products should be listed first where a consumer had entered the trademark as the search term, and fair competition should be ensured between branded products and private label products. They highlighted that consumers should have greater control over the influences shaping the choices available to them and should see the lowest prices available.

3.28 Other respondents suggested expanding the description of harm caused by ranking and recommendation algorithms to include indirect harms resulting from the incentives they create for companies to pursue bad practices. For example, a platform's endorsement for a product on a highly competitive marketplace could incentivise the use of fake reviews to achieve that endorsement. Honest firms and consumers would be negatively impacted by this if the platform had ineffective oversight mechanisms to detect fake reviews.

Collusion

3.29 Respondents considered that, for hub-and-spoke collusion, a series of vertical agreements between a hub and various spokes could be viewed illegal coordination among the spokes in circumstances where the hub was used as a means to indirectly communicate commercially sensitive information between them.

3.30 On tacit collusion, respondents noted that the definition of an 'agreement' would need to be considered in an algorithmic context, as would how to differentiate treatment of algorithmic and human interactions under the law. In addition, respondents noted that regulators would have to consider whether the designers of algorithms intentionally design them to learn to collude and to consider the role of intent in and of itself.

Harms respondents were most concerned about

3.31 In this section, we summarise responses related to our question: Are there specific examples that we should investigate further to consider whether they are particularly harmful and potentially breaching consumer or competition law?

Recommender Systems

3.32 In their submissions to the consultation, some respondents noted that the designers and deployers of recommender systems have substantial influence over consumers, particularly dominant firms.

3.33 Given their impact on consumers as well as citizens, some respondents suggested recommender systems be interrogated by the CMA and Ofcom within the remit of the Digital Regulation Cooperation Forum.

Ranking algorithms

3.34 Some respondents were particularly concerned about the use of ranking algorithms by large platforms to restrict access to customers. For example, in the case of comparison shopping sites, one respondent noted that competing service providers may have a reduced incentive to innovate in order to compete for user attention and loyalty, if ranking algorithms favour a platform's own shopping comparison service. This could reduce consumer choice and lead to increased costs if a lack of competition meant there was no downward pressure on prices.

3.35 In the online publishing sector, respondents noted that there was a lack of transparency about how platform's algorithms worked, the likely effects of changes made to them, nor was there warning given to publishers when changes were going to be made.

Pricing algorithms

3.36 Respondents considered that use of personalised pricing could increase in the future. Some were concerned about the effects on consumers of personalised pricing, saying that it should be banned in non-financial service sectors due to the detrimental impact on certain groups. Others considered that prohibiting the use of pricing algorithms would be excessive, however a more tailored response such as restricting the inputs into pricing algorithms could be a solution.

3.37 It was thought possible in theory that pricing algorithms could learn to collude autonomously, and that tacit collusion would be able to occur in a concealed way. Some respondents argued that dominant, technologically advanced firms could stand to gain the most from using such high-frequency pricing algorithms. Others thought that collusive agreements were less likely to succeed beyond automated price matching in the real world.

Specific examples of harms the CMA could investigate

3.38 Several respondents suggested that the CMA should investigate algorithmic pricing in general insurance markets. Concerns were raised about a lack of transparency around the data used to optimise prices for new customers and those renewing their insurance, and the inability of consumers to opt out of their data being used. They were also concerned that pricing practices in general insurance markets were leading to indirect discrimination, in contravention of equality law.

3.39 Some respondents also pointed to specific services for investigation. These included claims about YouTube's demonetisation of content (where content creators are denied paid advertisements on their videos, which are their primary revenue stream), such as the company's banning of certain words without a clear justification. Other claims related to unfair treatment of YouTube's Content ID system highlighted in a white paper by the Electronic Frontier Foundation. Content ID scans videos for copyright infringements by matching videos uploaded by creators to a database of files submitted by rightsholders. The claims included that for a given match that the system makes, the rightsholders can claim revenue from ads on the video in question, even whilst this action is being contested by the video creator. Beyond YouTube, there were also claims by some respondents about Amazon's practices of permitting counterfeit products to be sold by third-party vendors and only taking action in one jurisdiction (rather than all jurisdictions in which Amazon operates), and using its insider knowledge of third party vendor profits and margins to create cloned own-brand products.

Proposed investigation techniques to analyse algorithmic systems

3.40 In this section, we summarise responses related to our question: Are there any examples of techniques that we should be aware of or that we should consider beyond those that we've outlined?

Collecting and generating datasets

3.41 Respondents suggested the CMA gather datasets over time and use these for future inspections and investigations, as a way to create the required infrastructure for inspection.

3.42 Several respondents noted The Markup's Citizen Browser project as a good example of an auditing technique. The Citizen Browser is a custom web browser through which a nationally representative panel of paid users shares real-time data from their social media accounts with The Markup to form statistically valid samples of a population to understand how algorithms operate. This builds on the traditional 'mystery shopping' technique outlined in the CMA paper.

3.43 Another method of collecting data on consumer concerns that respondents proposed was through crowdsourcing from trusted websites, such as MoneySavingExpert. This could create an evidence base for concerns about particular companies that can only be surfaced by collating the testimonies of several consumers over time.

Accessing firms' data and code

3.44 Some respondents noted that, as highlighted in the CMA paper, APIs could give direct access to a firm's data. It was suggested that the CMA could draw inspiration from the telecommunications and computer networking industry to understand how this could work. However, others cautioned that both externally collated datasets and platform-provided APIs would be needed in order to enable independent verification of such firm-provided data access. Furthermore, API access would have to be agreed on an ongoing basis, and there was a risk that companies could manipulate data available to regulators through an API.

3.45 Respondents also highlighted tools used by other regulatory authorities to collect data from firms, such as the Financial Conduct Authority's RegData platform.

Going beyond technical approaches

3.46 Some respondents considered it important to go beyond technical approaches to inspecting algorithms in order to understand how an algorithm behaves. This could include reviewing the conception of the system, its commissioning, design, development, deployment, and ongoing use, as well as any subsequent assessment of its functioning. This review could include interviews with technical staff on product teams.

3.47 Others also highlighted that reviewing supporting business documentation could provide more accessible information to regulators than code or data. For example, documentation stored in a format that could be easily and quickly shared could give timely access to regulators and reduce the regulatory burden on the firm. Based on the review of documentation, the regulator could then decide to access the underlying data and code for a more technical analysis.

Challenges of the proposed techniques

3.48 Respondents noted there were several challenges to using the techniques proposed in the paper. Some of these challenges were centred around assumptions respondents perceived had been made in the CMA paper, for example that firms produce a final 'trained' algorithm, or that firms always retain training data once a model has been trained, which could be analysed during an inspection. They noted that this was often not the case. There was also a suggestion that regulation focus on outcomes rather than the specific AI technology used.

3.49 Other concerns included that some of the proposed techniques were either too superficial, such as mystery shopping, or too granular, such as accessing APIs, to reflect rapidly changing commercial realities. In addition, they noted that if many algorithms or algorithmic systems interoperate, inspection would become very challenging, raising the question of the level at which an inspection should be made, at the platform, algorithm, or other platform sub-system level.

3.50 There were also concerns around the proportionality of the investigation techniques relative to the harms to be investigated, such as the risks to privacy, trade secrets and user security.

Considerations for possible audits

3.51 Respondents highlighted several considerations for an algorithm audit, including differentiating between auditing the algorithm itself and auditing the controls over an algorithm, the latter of which are the organisational measures that can mitigate the risks associated with using algorithms. They also highlighted that much could be learnt from existing approaches to auditing, for example in financial services, for both internal and third-party audits.

3.52 Some respondents raised concerns about the assessment of liability and accountability in an audit. For example, if a small business asked a large social media platform to target certain customers with a discount, it may not be clear who would be accountable for possible discrimination or a lack of transparency. In another scenario, harm could be caused by humans (those creating, training, and adapting algorithms) rather than by the algorithm itself. Respondents noted that if the harm arose from the impact of the algorithm, that impact would have to be established with empirical evidence.

3.53 Another consideration was the need to clarify the purpose of the audit, to ensure end users or consumers would interpret it appropriately. For example, consumers should not assume that an algorithmic system’s fairness had been audited, when all that had been reviewed was how adequately the firm’s documentation described the system’s inner working.

3.54 Other considerations suggested by respondents included that any analysis of algorithms could begin with the results of pre- and post-launch testing, as well as oversight and scrutiny of the quantity, quality, standard, origin and necessity of the data used.

Role of regulators

3.55 In this section, we summarise responses related to our question: Is the role of regulators in addressing the harms we have set out in the paper feasible, effective and proportionate?

Whether existing laws are sufficient to address algorithmic harms

3.56 Several respondents considered that, overall, existing law could address many algorithmic harms. Some noted that, where a type of conduct was already prohibited by law, but its application to algorithms was novel, guidance could be issued to businesses to prevent the conduct from occurring by reference to the applicable existing law. Where there may be gaps, it was suggested that the CMA could run a consultation on clarifying expected market standards, or how the existing competition, consumer and data legislation applies to algorithmic practices. For example, some respondents noted that a precise definition of an algorithm would help to differentiate between applications where an algorithm enables a harmful practice, and applications where algorithms simply augment the ability of a human to make decisions.

3.57 On algorithmic collusion, there were mixed responses regarding whether existing laws could address the various types. Some considered that existing law could address potential horizontal price-fixing issues, and given that most algorithms are programmed by humans, they would be covered by companies' governance and oversight frameworks. However, others thought it might be necessary to rethink the basis of antitrust laws when it comes to autonomous collusion by algorithms, as focussing on communication between competitors with collusive intent and conduct would be difficult in a context where communication between humans is absent.

3.58 Some respondents identified several applicable laws for personalised pricing, as laid out in a paper by Ofcom, 'Personalised pricing for communications'. These included the Data Protection Act 2018, the Consumer Protection from Unfair Trading Regulations 2008, Unfair Terms in Consumer Contracts Regulation, the Consumer Rights Act 2015, the Competition Act 1998, the Enterprise Act 2002, and the Equality Act 2010. Respondents also highlighted that the Platform to Business regulation ensured a level of transparency to business users.

3.59 On liability, respondents noted that liability could arise only from conduct that is committed 'intentionally' or 'negligently'. This posed a challenge for algorithms that do something the designer did not anticipate they would do. Some suggested that application of the precautionary principle could cover the risks that arise in such instances. Others noted that users of algorithms that they have not themselves developed should be able to rely on statements and, where appropriate, warranties and indemnities provided by developers so as not to be held liable for consequences of which they were unaware and against which they took all reasonable steps to avoid.

Prioritising harms for the CMA to investigate

3.60 Respondents commented that harms for investigation could be prioritised by several factors, including their impact and frequency or likelihood, for which empirical evidence would be required to be able to quantify each factor before intervention is considered. Indeed, some noted that a threshold would need to be established to create a minimum standard for intervention. Further, guidance would help firms understand how each harm would be assessed and enforced and which regulatory regime would apply in each case.

3.61 Others suggested that the focus should remain on algorithmic systems themselves, rather than on harms related to self-preferencing or choice architecture, which they considered to be tangential. They noted that benefits should also be carefully weighed against harms before intervention.

Cooperation with other regulators

3.62 Several respondents emphasised the imperative for the CMA to work together with the ICO and Ofcom, such as through the Digital Regulation Cooperation Forum, to ensure regulatory coherence and avoid duplication. These regulators could work together to develop the appropriate regulatory regime and share their expertise on topics such as adtech, online fraud and scams, misleading information, recommendation and collaborative filtering algorithms, and establishing the boundary between the consumer and the citizen. In all these areas, they noted that system design decisions should be at the focus for regulators.

3.63 Regulators that have existing expertise or competence in an area should take the lead, according to some respondents. There should also be consistency in approach to auditing algorithms, including investigatory techniques and information gathering, to ensure firms disclose information in a consistent way across regulators. Respondents also thought it was important for other regulators to have equivalent inspection and audit powers to the Digital Markets Unit, to ensure that the UK’s digital regulatory regime is not disjointed.

3.64 Respondents cautioned that the financial services sector is already heavily regulated, and it would therefore be important to avoid any additional rules that duplicate or conflict with existing rules. Some also warned that it would be risky to take regulatory inspiration from the financial service sector. They noted that the Financial Conduct Authority's approach has been to limit the scope of sector-specific regulation, rather than to extend it. There could therefore be negative consequences if the CMA were to extend a form of financial services-type prudential or conduct regulation to the use of algorithms in all sectors.

3.65 Beyond other regulators, respondents thought the CMA should coordinate with other parts of government responsible for data driven systems, such as DCMS, the Office for AI, the Cabinet Office, and the Office for Statistics Regulation. Other respondents also suggested the CMA collaborate with industry to test regulatory efforts and co-create governance frameworks through policy prototyping or sandbox activities. While the CMA could set the objectives, companies could make proposals to achieve those objectives, making use of their technical expertise.

Evidence gathering

3.66 Several respondents noted the need to consider the protection of trade secrets and intellectual property, and the cost to firms of providing information, when requesting evidence from firms, urging a proportionate approach.

3.67 Some also noted the need to take into account the algorithmic explainability requirements of other regulatory authorities when making requests, to minimise unnecessary complexity and maximise coherence between regulators' approaches. Transparency obligations would also need to set reasonable expectations and leave room for continuous improvement and evolution of algorithms. Some noted that explanations under any new regulatory intervention should be sufficiently detailed to promote education, but not so detailed that they must be updated and evaluated continuously.

3.68 Respondents also highlighted that the CMA would need to be sufficiently resourced to ensure that the threat of detection of non-compliance was too high for firms to take the risk, and suggested taking inspiration from the Environment Agency's "Operator Monitoring Assessment". They noted that schemes such as this combine both a carrot and stick for enforcement.

Requirements and guidance the CMA could produce

Disclosure of information

3.69 Respondents suggested that organisations could be required to regularly publish statistics on topics such as the evolution of their algorithms, bias levels, and false positive and false negative rates.

3.70 Developers or controllers of algorithms could also be held accountable, if not liable, for the choices they make in developing and deploying algorithms by requiring transparency and explainability of automated systems. Some respondents also suggested that requiring appropriate disclosure, based on use-case and end-user, should be the default expectation for companies creating, distributing and commercialising AI systems. Transparency could also be encouraged through open registers of algorithmic systems, such as the Amsterdam Algorithm Register for city authorities that can be inspected by the public. A national register could focus on firms of a certain size or sales volume.

3.71 Respondents also suggested that the CMA could have pre-emptive powers including access to the full range of relevant documentation of an algorithmic system development project. If this was lacking, an ethical audit could be mandated as a standard part of any development process. Beyond this, the CMA could look into algorithmic system before they are deployed to ensure they do not adversely affect vulnerable consumers, in a similar way to which planning permission is required before building a house.

Use of data

3.72 Respondents noted that guidance should be produced on whether it is appropriate to allow commercial use of special category data or to draw inferences about a person's health or sexuality for commercial purposes.

3.73 Guidance would also be required on how firms could show they had found and mitigated bias in their datasets.

How the CMA will enforce competition and consumer law

3.74 In the context of procuring an algorithmic system from a third-party, respondents noted that clarity was needed on what an 'informed purchase' means when purchasing an algorithmic system. Further, although large entities would be required to share certain information with buyers as part of procurement rules, respondents noted that guidance was needed around how competitive companies could show they had followed various guidelines, to ensure they were not undercut by other companies that took shortcuts. This could be supported by requiring disclosure of standardised information about how algorithms are developed or trained, as well as checks for known biases or equalities issues. Moreover, respondents noted that authorities may need to find mechanisms to ensure that companies do not base their business models on datasets they have acquired illegally.

3.75 Respondents also noted that timely and targeted enforcement would create credible deterrence and improve compliance with the law. They also suggested that the CMA's decision not to conduct a market investigation into the online platforms and digital advertising sector could have signalled to the industry that consumer protection and competition law would not be enforced to the highest standard in the UK.

3.76 Some respondents considered that regulators could define clear benchmarks of algorithmic accountability that would act as a minimum level of self-policing firms are required to do. This would help firms to fulfil their duty to undertake due diligence under antitrust law. Further, a ‘safe’ list of lawful and acceptable algorithmic systems, alongside a ‘no go list’ of use cases that are clearly unfair or anti-competitive, developed in consultation with stakeholders, could provide positive incentives for companies to use compliant systems.

Research into development of auditing tools and compliant algorithms

3.77 Respondents commented that the CMA could encourage others in academia and industry to produce tools, including open-source tools, to audit algorithmic processes affordably. This could be done through competition and bounties, or research funding in collaboration with public funding bodies.

3.78 Research could also be done into algorithms that comply with competition and consumer law, which could incentivise platforms to use compliant algorithms over those that may not be compliant.

Development of standards

3.79 In considering the description of harms overall, some respondents discussed the incentives on firms to practice good governance. For example, some noted the difference between firms that are incentivised to maximise long-term user satisfaction, and those that depend on one-shot interactions with consumers, prioritising short-term revenue gains. They suggested that the CMA should encourage firms to adopt high governance standards in addition to proactively identifying harms through technical means.

3.80 Respondents suggested a number of standards could be developed and certified using audits. These standards could mitigate against defects in the software used and the competence of staff developing algorithms, loss of database integrity, defective model ethics, defective model training, and inadequate understanding and framing of the requirements of the application's stakeholders. Guidance could be provided for firms on how to meet these standards and could be aligned to other relevant government policy.

Other ideas or approaches the CMA should consider as part of its role

Protecting vulnerable consumers

3.81 Several respondents highlighted the need to consider nuances in protecting vulnerable consumers. For example, these included widening protected characteristics to include low-income households. Research by Citizen's Advice (2018) found that some low-income consumers disengaged from the insurance market when faced with personalised pricing because they recognised that they were likely to get a higher premium for things like car insurance based on their profile. Other respondents also noted that vulnerability needed to be categorised more granularly to include explicit mention of children, those with learning disabilities, people lacking digital literacy, and other disadvantaged groups.

3.82 Other respondents noted that in order to protect vulnerable consumers, it was important to enable firms to use protected characteristics as inputs into algorithmic systems, so that vulnerable people could be protected from fraud and offered tailored customer support.

Appendix A: List of formal respondents

1. Ada Lovelace Institute
2. American Bar Association
3. British Brands Group
4. British Computing Society
5. Bruce Wardhaugh (University of Manchester)
6. Carnegie UK Trust
7. COFECE
8. Competition Law Forum
9. Deloitte
10. DMG Media
11. European Competition Lawyers Forum
12. Facebook
13. Fairer Finance
14. Google
15. IBM
16. Jennifer Cobb and Jat Singh (University of Cambridge)
17. Just Algorithms Action Group
18. Kelkoo
19. Law Society of Scotland
20. medConfidential
21. Nicolo Zingales (FGV Direito Rio)
22. Nik Lomax and Stephen Clark (University of Leeds)
23. Ombudsman Services
24. Regulatory Institute

25. Reset

26. Santander

27. techUK

28. Timo Klein (Utrecht University/Oxera)

29. Uber

30. UK Computing Research Community

31. UK Finance

32. UKRI Trustworthy Autonomous Systems Hub

33. Which?

34. Yoti

35. Zach Brown (University of Michigan) and Alexander MacKay (Harvard University)