Response to the Competition and Markets Authority Call for Information:

Algorithms, Competition and Consumer Harm

Submitted by Prof. Derek McAuley, Prof. Tim Norman, Prof. Peter Cartwright, Prof. Richard Hyde, Dr. Elvira Perez Vallejos, Dr. Enrico Gerding, Dr. Sebastian Stein, Dr. Ansgar Koene, Dr. Murray Goulden and Dr. Jiahong Chen

16 March 2021

1. The UKRI Trustworthy Autonomous Systems (TAS) Hub assembles a team from the Universities of Southampton, Nottingham, and King's College London. The role of the TAS Hub is to coordinate and work with six research nodes to establish a collaborative platform for the UK to deliver world-leading best practices for the design, regulation and operation of 'socially beneficial' autonomous systems. The team share the vision that to realise the industrial and societal benefits of autonomous systems, they must be trustworthy by design, judged both through objective processes of systematic assurance and certification, and via the more subjective lens of users, industry, and the public.

2. The UKRI-funded Horizon Digital Economy Research Institute centred at the University of Nottingham brings together an interdisciplinary team with expertise from a wide variety of backgrounds including computer science, engineering, mathematics, psychology, sociology, business, social science and the arts. The team is addressing the research challenge of how to promote deep personalization, whilst providing control and privacy to citizens, even as we develop new blended experiences that converge traditional and digital artefacts, services and media.

3. We welcome the CMA's publication of the research paper *Algorithms: How They Can Reduce Competition and Harm Consumers*, which outlines the various categories of harms that algorithmic systems could pose to consumers and the digital economy. In response to the consultation questions below, we aim to provide further evidence and perceptions based on our research to support the CMA in understanding the current landscape and making decisions on the next steps.

Question 1: Are the potential harms set out in the review paper the right ones to focus on for our algorithms programme? Are there others that we have not covered that deserve attention?

4. The research paper has identified a wide range of harms to consumers and competition caused by uses of algorithms. We agree that these are all important and urgent matters that the CMA should address, but would also like to point out certain harms that have not been explicitly covered by the paper in full:

5. **Negative psychological impacts.** With empirical evidence, our research (Pérez et al, 2021) has shown that algorithmic decision-making processes can cause negative impacts on the mental well-being of young people.[1] These impacts include, but are not limited to, those around online privacy,

[1] https://doi.org/10.1177/1460458220972750

safety and trust, as well as excessive screen time and related social isolation problems. Online algorithmic systems can aggravate these impacts by targeting users with highly revealing data. The so-called 'interest-based' approach in the online advertising and social media sector, based on fine-grained behavioural and demographic data about users, can create highly addictive personalised content. Findings from our engagement with young people (Creswick et al, 2019) also show that do not necessarily have enough awareness or knowledge of such harms, or even show a strong sense of resignation,[2] making it even more difficult to investigate the impact of algorithmic systems on them.

6. **Overcollection and oversharing of consumer data as a harm *per se*.** In Section 2.1 the paper outlines four kinds of direct harms algorithmic systems can cause, which are certainly enabled or exacerbated by the collection and sharing of personal data about consumers. However, it is worth pointing out that even *without* these harms, overcollection and oversharing of data can be detrimental to consumers by widening the informational and power asymmetries between traders and consumers. While it is true that conducting market research has always been an acceptable business practice, the use of consumer data facilitated by algorithmic systems makes market insights more accurate, more available, and sometimes more intrusive. As a result, businesses as a whole will gain an increasingly significant informational edge over consumers compared to pre-algorithmic days, arguably breaking the informational equilibrium and power balance between traders and consumers. Our research (Cartwright, 2015) has highlighted the risks associated with the 'informational vulnerable', especially consumers who have restricted capacity to understand the role of advertising or product effects.[3] This also echoes the Furman report's position that indirect impacts on consumers are not just always about costs.[4] It should be noted that this is not a regulatory matter exclusively for data protection authorities, because such harms can emerge without violating data protection law, and they can also constitute aggressive commercial practices depending on the details of specific cases, especially when undue pressure is involved.[5] Higher-level consumer welfare, especially in digital markets, should be monitored closely and constantly by the CMA.

7. **Discrimination against certain socio-economic groups.** Section 2.1.3 draws heavily on equality law, which we agree is a great challenge that the CMA should look into. However, as some of us have previously submitted,[6] regulators should also begin to consider discriminatory practices beyond protected characteristics, and to also cover discriminatory practices based on socio-economic categories. Section 1 of the Equality Act 2010, which would impose a statutory duty on public authorities to reduce socio-economic inequalities, is currently in force only in Scotland and not the rest of the UK. Nevertheless, the role of algorithms in surfacing and intensifying socio-economic inequalities is a crucial matter for consumer welfare and should be further investigated as part of the CMA's long-term strategies. The controversies around GCSE and A-Level grading last year have underlined how the public may reject algorithms not only on grounds of measurable accuracy, but also for the very opposite reason: because they can i) lock-in pre-existing disparities, further entrenching inequalities and preventing social mobility, and ii) do so in an overt manner which draws

[2] https://doi.org/10.1108/JICES-11-2018-0090
[3] https://doi.org/10.1007/s10603-014-9278-9
[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf
[5] https://www.i-law.com/ilaw/doc/view.htm?id=262490
[6] https://doi.org/10.17639/9M8B-9P34

attention and thus demands accountability. To take the school gradings example, it is widely acknowledged that private schools confer advantages on their pupils, but it was only when such disparities were hard coded into the grading algorithm that public acceptance was lost. In this regard, the real challenge for the acceptability of algorithmic systems is not creating 'accurate', 'value-free' systems (Chen, 2018)[7] – which will only reflect and reinforce an empirically anti-meritocratic status quo – but taking anticipatory, proactive steps to ensure those systems are designed to promote a fairer, more inclusive and more diverse society in the first place.

8. **Selective withholding of data as an abuse of market dominance.** Data generated in the process of operating digital services, whether personal or non-personal data, can be highly valuable to all players in the market. Such data, however, is not always made available to the business users of the service, raising questions about the fairness of this practice, especially when the data collection was possible only when the business user or its end-users were involved in the first place. Dominant businesses may take advantage of its control over the data, as well as the underlying infrastructures, to share data only to certain partners, creating detrimental effects to other competitors. This process can be facilitating by algorithmic systems, leading to worsened market distortions. At the moment, the EU is considering regulating this practice with the proposed Digital Markets Act,[8] something UK regulators should also consider. We would also like to point out that, considering how individual consent has been abused by service providers, relying on consent is unlikely to be a helpful way forward, as consumers are susceptible to 'choice architecture', leaving much room for manipulation that would lead to over- or under-sharing of their data with third parties.

Question 2: 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?

9. While we agree most of the harms described in the paper have reflected the scope and nature of the associated practices, some of them can be framed more broadly to cover some emerging trends.

10. From **'self-preferencing'** to **'differentiated treatment'**. Graef (2019) has conceptualised three forms of differentiated treatment in platform-to-business relations, including pure self-referencing, pure secondary line differentiation, and hybrid differentiation.[9] The self-preferencing practices depicted in the paper covers mainly the first category but not the other two. It is important to note that offering differentiated treatments among non-affiliated business users based on, for example, the amount of fees, can nevertheless create anti-competitive effects. Such practices should be included in a broadened description of the harms.

11. From **'vulnerabilities'** to **'susceptibilities'**. In Sections 2.1.1 (price personalisation) and 2.1.2 (non-price personalisation), the paper has pointed out that personalisation can be particularly problematic for consumers with vulnerabilities or protected characteristics. While we share the concerns about these potential harms, we equally feel that exploitations can also take place against consumer traits that are beyond protected characteristics and typically-defined, intrinsic vulnerabilities, such as those related to age or disabilities. Our research on the taxonomy of consumer vulnerabilities (Cartwright, 2015) provides a helpful framework for identifying practices of

[7] https://doi.org/10.21552/edpl/2018/1/7
[8] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:842:FIN Art 6(1)(a)
[9] https://doi.org/10.1093/yel/yez008

exploiting such vulnerabilities, notably informational vulnerability, pressure vulnerability, supply vulnerability, redress vulnerability and impact vulnerability.[10] Spencer (2020) has also outlined how online manipulation can take the form of exploiting user insecurities, weaknesses, biases and vulnerabilities, or even worse, *creating* these susceptibilities and *then exploiting* them.[11] These aspects about users are not necessarily classified as vulnerabilities as such but can be equally detrimental to consumers. We suggest using a broader term 'susceptibilities' and giving further examples to highlight these more subtle, contextual harms. It should also be noted that such tactics do not always involve mis/disinformation or deception, making it harder for regulators to intervene under the current consumer protection legal framework.

Question 3: How likely and impactful are the identified harms now, and how might they evolve in the next few years?

12. The harms in relation to algorithmic systems that have been identified in the paper are largely taking place in the 'online' (i.e. internet) setting, but as IoT technologies become more popular in smart homes (e.g. smart speakers), transport (e.g. autonomous or connected vehicles) and workplaces (e.g. smart office), these harms may replicate and evolve in these connected environments in the coming years. Regulators should take a more anticipatory approach to pre-empt the potential harms with regard to B2C and C2C e-commerce activities based on the IoT.

13. The increasing number of user interactive points associated with the fast-expanding IoT sector provides not only an exponentially growing amount of data, but also unprecedentedly more ways to influence consumers with algorithmic systems. For example, advertising outside the internet, such as in a smart city in the near future, enabled by state-of-the-arts technologies such as physical tracking and facial recognition, is already being explored by the industry. Some of the risks in regard to these developments have been identified in our research (Schraefel et al, 2020).[12] Another example is connected vehicles, whose ability to collect a variety of data will not only have surveillance implications, but also bring into question the ethicality of the use of such data by, say, the insurance sector.

14. Currently, the lack of platforms in the IoT economy may also lead to consumer lock-in. Personal information management systems (PIMS) may provide a market-based solution in the IoT context, but our research (Urquhart et al, 2018) has highlighted certain technical, legal and commercial barriers, which could be intensified with sophisticated algorithms.[13]

Question 4: Are there specific examples that we should investigate further to consider whether they are particularly harmful and potentially breaching consumer or competition law?

15. No answer.

[10] https://doi.org/10.1007/s10603-014-9278-9
[11] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341653
[12] https://doi.org/10.4337/9781788972000.00012
[13] https://doi.org/10.1007/s00779-017-1069-2

Question 5: Are there any examples of techniques that we should be aware of or that we should consider beyond those that we've outlined?

16. Our work (Gunes et al, 2019) has highlighted the importance to addressing vulnerabilities of AI algorithms with regard to data sources as well as exploitation of the algorithms.[14] In relation to data sources, further strategies can be found in Gunes et al (2019),[15] Biggio et al (2012),[16] and Baracaldo et al (2017, 2018).[17] In terms of exploitations, see Gunes et al (2019),[18] Alzantot et al (2018)[19] and Carlini et al (2016).[20] We also call for the investment in developing trusted datasets that are carefully curated and reflective of diversity and inclusiveness for development and testing of algorithmic systems.

Question 6: Are there other examples where competition or consumer agencies have interrogated algorithms that we have not included?

17. No answer.

Question 7: Is the role of regulators in addressing the harms we set out in the paper feasible, effective and proportionate?

18. While the role of regulators set out in the paper is appropriate, the effectiveness of these strategies would depend on timely and targeted enforcement actions. As some of us have previously submitted to the CMA, a market investigation could help collect evidence in an independent and objective manner and create deterrence to non-compliant commercial behaviour.[21] Our research (Cartwright, 2014) has demonstrated how responsible enforcement actions can create 'credible deterrence' that would improve compliance.[22] The CMA's decision not to conduct a market investigation into the online platforms and digital advertising sector could have released a signal to the industry that consumer protection and competition law would not be enforced to the highest standard in the UK. In parallel to the anticipation of the establishment of a new cross-sector digital market regulator, the CMA should also take timely actions against anti-competitive practices.

Question 8: Are there other ideas or approaches that we should consider as part of our role?

19. One challenge in regulating algorithmic systems to minimise their harms is that the line between acceptable and unfair uses of these systems can be extremely hard to draw. The definitional difficulties in outlining the scope of online manipulation, for example, are widely recognised.[23] Therefore, instead of focusing on the borderline, hard cases, regulators could consider a list-based

[14] https://doi.org/10.24963/ijcai.2019/44
[15] https://doi.org/10.24963/ijcai.2019/44
[16] https://arxiv.org/abs/1206.6389
[17] https://doi.org/10.1145/3128572.3140450; https://doi.org/10.1109/ICIOT.2018.00015
[18] https://doi.org/10.24963/ijcai.2019/44
[19] https://arxiv.org/abs/1804.07998
[20] https://dl.acm.org/doi/10.5555/3241094.3241135
[21] https://www.horizon.ac.uk/wp-content/uploads/2020/12/PDF-12.pdf
[22] https://www.taylorfrancis.com/chapters/credible-deterrence-consumer-protection-imposition-financial-penaltieslessons-financial-conduct-authority-peter-cartwright/e/10.4324/9781315867663-3
[23] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2565892

approach as part of the role in providing guidance as set out in Section 4.1. These would involve, after consulting consumer groups, civil society organisations, experts and the industry, drawing up a 'safe list' with typical uses of algorithmic systems that are clearly lawful and widely considered acceptable, so as to create compliance incentives for businesses to adopt these solutions. At the same time, a 'no go list' should also be set up to underline the use cases that are clearly unfair or anti-competitive. Following the departure from the EU, the UK has now greater flexibility to amend Schedule 1 of the Consumer Protection from Unfair Trading Regulations 2008 if practices which were regarded as always unfair can be identified. As noted in the paper, traders in the UK have a general duty not to trade unfairly and act in accordance with the requirements of professional diligence, which covers more than misleading and aggressive practices. The wide range of examples of algorithmic harms identified in the paper may provide a helpful basis for such an approach.