Response to the Government's Consultation

Smart Data: Putting Consumers in Control of Their Data and Enabling Innovation

Submitted by Prof. Derek McAuley and Dr. Jiahong Chen of
Horizon Digital Economy Research Institute, University of Nottingham

6 August 2019

1. Horizon[1] is a Research Institute centred at The University of Nottingham and a Research Hub within the UKRI Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives, specifically related to opportunities and challenges in personal data use. Prof. McAuley is director of Horizon and was a member of the Furman Digital Competition Expert Panel for HM Treasury that published the "Unlocking Digital Competition" report. Dr. Chen is a Research Fellow of Horizon, currently working on the EPSRC-funded DADA[3] (Defence Against Dark Artefacts) project, addressing smart home IoT network security, and its acceptability and usability issues.
2. This response is submitted in our personal capacity, and we are happy to be contacted at derek.mcauley@nottingham.ac.uk and jiahong.chen@nottingham.ac.uk.
3. We are happy for our response to be published and shared with the Competition and Markets Authority, the Financial Conduct Authority, Ofgem, Ofcom, the Information Commissioner's Office, and the Money and Pensions Service.

1. Do you agree with the proposed objectives and expected benefits of Open Communications? Are there any other benefits or risks that we should consider?

4. We agree that, by requiring sharing of customer and product data to TPPs, Open Communications has the potential to achieve its objectives of stimulating innovation and improving outcomes for consumers. Such policy goals should however also highlight more specifically the importance of promoting competition, consumer choice and data protection in the communications sector. In line with these objectives, a number of potential risks should be taken into consideration when implementing Open Communications in order to maximise its benefits:
5. Competition: While mandatory sharing of data is in principle considered an effective way to lower entry barriers for new services, policymakers should also assess the competition impact with regard to the concentration of consumer data by dominant players in the market, who might exploit Open Communications and further expand their grip on consumer data with pre-existing technical, resource and market advantages.

---

[1] http://www.horizon.ac.uk
[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/
[3] https://www.horizon.ac.uk/project/defence-against-dark-artefacts/

6. Consumer choice: Enabling TPPs to provide product comparison information to consumers and complete switching on their behalf, which forms an important part of the Open Communications proposal, will indeed play a key role in helping consumers make informed choices. This would however also depend on the accuracy of information and objectivity of recommendations provided by the TPPs, which might be affected by the quality of data, the reliability of algorithms, and the existence of business partnership with service providers. Potential abuse of platform power by TPPs may have serious anti-competitive effects and should therefore be treated with extra caution.

7. Data protection: We have concerns about TPPs' access to consumer data leading to the even more prevalent business model of monetising such data, which would run counter to Open Communications' objective of promoting consumer welfare. Policymakers should therefore consider providing regulatory incentives – or even requirements where necessary – to encourage TPPs to develop services or apps using modern Privacy Enhanced Technologies (PETs), for example offering product comparison or recommendations with the consumer data retrieved, stored and analysed locally on the client side, without giving direct TPPs direct access to such data. Risks can be minimised with end-to-end communication that does not involve the TPPs, but since such an arrangement is unlikely to be favoured by the provider,[4] a "carrot-and-stick" regulatory approach may be needed.

2. What is the most effective approach to implementation to ensure the success of Open Communications in enabling innovation and delivering the best consumer outcomes?

8. We agree that Ofcom is in the best position to lead the implementation of Open Communications, and welcome the Government's initiative to work closely with the industry and TPPs. However, to achieve a genuinely user-centric and user-friendly outcome, Ofcom should have consumer organisations, civil society groups, experts and other regulatory bodies (such as the CMA and the ICO) involved at an early stage of the design and implementation of Open Communications.

3. Are there any further actions we should take to enable consumers to benefit from Smart Data in regulated markets?

9. Our suggestion of encouraging TPPs to run their services on a more privacy-preserving business model, perhaps based on the use of PETs, with revenue from commissions instead of aiming to add to this income through monetisation of consumer data, applies not only to the communications sector. In other regulated markets, such as financial services and utilities, there is also a wide scope for TPPs to develop software or apps for consumer equipment (e.g. personal computer, in browser, smartphones, and smart appliances), that access consumer data directly from the sources without storage or reuse of individual consumer data on their servers.

4. In which other markets, outside of the regulated and digital markets, would there be the greatest benefits from Smart Data initiatives? Please explain your reasoning

10. No response.

[4] The Royal Society, "The Internet of Things: opportunities and threats", p8. https://royalsociety.org/-/media/events/2017/10/tof-iot/iot-conference-report-final.pdf

5. What other roles might industry find it useful for Government to perform in addition to it acting as a facilitator for Smart Data?

11. At an early stage of the development of Smart Data in a particular sector, maintaining a facilitating role would be helpful to stimulate innovation without excessive compliance burdens on start-ups. However, past experiences have shown that, while interoperability has emerged spontaneously in certain sectors (e.g. email standards), it sometimes takes regulatory intervention to achieve coordination in other sectors (e.g. mobile number portability).[5] It is therefore important for the Government to review the developments in different sectors on a regular basis, and where necessary, to take stronger actions in co-regulating Smart Data in those fields, including providing additional incentives, setting out stricter conditions for merger approvals, or even mandating statutory portability requirements. Such measures, if defined proportionately and implemented properly, would have a positive impact on the healthy growth of the market and a level playing field for the industry.

6. Do you agree that we should establish a cross-sector Smart Data Function with the proposed responsibilities set out above?

12. We would like to underline that the approach taken in implementing Open Banking has proved largely successful and can serve as an example for future initiatives in other sectors. Considering the divergence of the needs, challenges, and regulatory environment unique to each individual sector, sometimes a sector-specific approach may be more effective and efficient.

13. Having said that, we also see the benefits of setting up a cross-sector Smart Data Function when there is a need for developing cross-sector interoperability or integrating existing Smart Data systems across sectors. In addition, maintaining a cross-sector unit may reduce duplicate costs for coordinating and administrating specialised teams for rolling out Smart Data to new markets. The efficiency of the Function, however, will depend mainly on their ability to build up a dynamic team capable of tackling sector-specific issues (or cross-sector issues, depending on the aim of a particular action) by involving stakeholders, experts and regulatory bodies relevant to the market concerned.

7. What would be the best form for the Smart Data Function to take? Should it be, for example, a new body, part of an existing body or some other form?

14. Accordingly, instead of setting up a full-scale unit to cover all potential sectors with a large number of permanent staff, the Smart Data Function should take a relatively light-weight organisational form and primarily a coordinating role. When the need to adopt Smart Data emerges in a particular area, a working group can be set up to implement Smart Data in that area, with administrative and logistic support from the Function.

[5] See "Unlocking digital competition Report of the Digital Competition Expert Panel", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf, p5.

8. How can we ensure that the costs of Smart Data initiatives are shared fairly between the participating businesses?

15. The approach outlined above would also allow for flexible, sector-specific arrangements for sharing costs between participating businesses. In sectors where there is a strong industrial motivation to push forward the Smart Data initiative, the costs can be shared by the industry, including service providers and TPPs. In other sectors where such a motivation is lacking, the Government should consider either making use of public funds or attracting private investors (for example, with various models of PPP[6]) to carry out the development of the necessary technologies and standards.

9. What other actions could the Government or regulators take to support the use of data and innovative services to improve outcomes for vulnerable consumers?

16. The Government should encourage data and innovative service to take into account the special needs of vulnerable consumers. This includes, for example, designing services in ways compliant with the principle of "data protection by design and by default"[7], whereby privacy-preserving options are enabled by default (e.g. permission to perform on device data processing but no sharing), so users with vulnerabilities do not need to change such settings to receive protection.

10. Should we strengthen the powers of sector regulators to enable them to use consumer data to improve their understanding of the challenges faced by vulnerable consumers and to intervene to improve outcomes?

17. As much as we support the Government's initiative to help regulators improve their understanding and intervention for vulnerable consumers, access to the data, in particular when it comes to data about consumers with vulnerabilities, should be performed only when it is necessary and fully in line with all data protection principles, including having a lawful basis, such as consent. In fact, research activities in public interest are already benefiting from certain derogations provided by data protection law.[8] Such possibilities should be fully considered before any attempt to confer further broad data access powers to sector regulators.

11. How can we ensure that the Smart Data Function improves outcomes for vulnerable consumers? Do we need to consider any further actions?

18. We welcome the Government's commitment to place vulnerable consumers at the heart of the Smart Data Function, who should, following the operational model we suggested in Paragraphs 12-15 above, provide general guidelines to help various working groups identify the special needs of vulnerable consumers and avoid the common pitfalls that might compromise their interests. In assessing whether (co-)regulation is needed in a particular sector, the Function should also take utmost account of whether industry initiatives have sufficiently addressed the needs of vulnerable consumers – mostly to date they do not.

---

[6] Public-private partnership, whereby, in some models for example, private investors are contracted to build the infrastructure, and in return, they are granted the right to charge the users of the infrastructure.

[7] See DPA 2018, Section 57; GDPR, Article 25.

[8] See DPA 2018, Section 19; GDPR, Articles 5(1)(b), (e), 9(2)(j), 14(5)(b), 17(3)(d), 21(6), 89.

12. Do you agree these protections for when TPPs use Smart Data are needed? Are there others we should consider?

19. We agree that all the proposed safeguards are necessary for protecting consumer data. In addition, and as highlighted above, Smart Data initiatives should always encourage or even require TPPs to develop services that are privacy-preserving and friendly. Many of the existing and potential TPP services can be run in such a way that consumer data is analysed on the user's terminal device, without sharing data to the TPPs themselves. Our ongoing research project, Databox,[9] has proved this approach is both technically and commercially feasible in an IoT setting, and we do not see any reason this model cannot be followed in other markets (e.g. media[10]). When developing the Smart Data infrastructures, policymakers should take actions to ensure this approach is technically supported (e.g. data interoperability with terminal devices and apps) and commercially incentivised (e.g. by reducing compliance burdens for services adhering to this model).

13. How should our proposed approach to accreditation operate in practice if it is to effectively ensure that consumers' data are protected and minimise burdens for TPPs?

20. The current data protection legal framework has already laid down the general principles and mechanisms for the operation of certification schemes and accreditation procedure.[11] The ICO has been working on setting out the criteria for the certification scheme in the UK.[12] The accreditation of TPPs for Smart Data initiatives can be aligned with the data protection certification scheme, with selected certification bodies also empowered to review accreditation applications from TPPs. This will not just minimise unnecessary extra costs for setting up a separate accreditation authority but will also reduce compliance burdens for TPPs. Most importantly, this will ensure accreditation decisions are subject to a set of criteria consistent with existing data protection standards.

14. What are the advantages and risks of introducing a cross-sectoral general authorisation regime for TPPs?

21. The proposed cross-sectoral general authorisation regime will enable TPPs to conduct business in multiple markets, and potentially to link consumer data from across various sources and generate highly revealing profiles. For this reason, the competition, consumer choice and data protection risks, as outlined above in Paragraphs 5-7 above, will be even more likely to materialise. Again, developing an environment of privacy-preserving use of consumer data is crucial, and where necessary, policymakers should consider setting out limits on cross-sector data merger to maintain a degree of data separation, possibly even mandating the strong isolation provided by PETs.

---

[9] https://www.horizon.ac.uk/project/databox/

[10] For instance, see BBC Box: https://www.bbc.co.uk/rd/blog/2019-06-bbc-box-personal-data-privacy

[11] See DPA 2018, Section 17; GDPR, Articles 42-43.

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/certification/

15. What other options should we consider to ensure that consumers are protected when using TPPs?

22. When developing the technical framework for sector-specific or cross-sector Smart Data initiatives, certain data protection functionalities and safeguards should be built into the system, which may include, for instance, a robust identity verification system (e.g. UK Verify[13]), compulsory logging of data sharing activities and traceability of data uses, and a one-stop-shop or dashboard-like platform for consumers to review data sharing reports and where necessary, stop data sharing to some or all TPPs.

[13] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify