Written evidence submitted by Dr Ana Canhoto, Professor Ashley Braganza and Dr Asieh Tabaghdehi

DCMS Committee

Connected tech: smart or sinister?

Evidence submitted by Dr Ana Canhoto, Professor Ashley Braganza, & Dr Asieh Tabaghdehi (Centre for Artificial Intelligence: Social and Digital Innovation; Brunel University London)

Short bio

Our response is a collective effort, compiled by three academics based in Brunel University London:

Ana Canhoto, Reader in Marketing. Her research focuses on the use of digital technology in interactions between firms and their customers, including obtaining customer insight from social media, and AI-enabled personalisation. She leads the "Innovation, Digitalisation and Society" research lab.

Ashley Braganza, Professor in Business Transformation. His research interests encompass big data, change management, strategy implementation, process and knowledge management, and transformation enabled information systems. He is co-director of the Centre for AI: Social and Digital Innovation.

Asieh Tabaghdehi, Lecturer in Strategy & Business Economy. Her current research expertise lies in digital economy with the focus on ethics for AI, digital footprint data and SMEs digital adoption in digital ecosystem. She leads the BSc International Business Programme.

June 2022

Executive summary

- The most important impact of smart technology has been the datafication of daily life, which creates opportunities, as well as threats, at the individual, organisational and town levels.
- Vulnerability in the face of smart technology arises from contextual factors, such as unavailability of technology, inability to technology, and consequences of using technology.
- To design socially responsible smart technologies, firms need to consider how the connectivity, cognitive ability and imperceptibility of the smart system create specific risks in terms on input, process, and output. This can be enforced through a mixture of push and pull mechanisms.

- Smart technology can fundamentally change the nature of competition in its associated industries. There are also important risks to consider at the level of individuals' safety and their mental health.
- Customers are unlikely to make purchase decisions of smart technology based on geo-political considerations.

———————————————

1. **What has been or will be the most important impacts of increasingly prevalent smart and connected technology in our lives, including in the home, in the workplace and in our towns and cities, and are they necessarily better**

Are there any groups in society who may particularly benefit from or be vul Td ( )Tj

applied only after a problem is evident (e.g., fatalities caused by self-driving cars).

3.2.　　A better approach is to identify the value destruction potential of the technology, before it is deployed. This is done by firstly, mapping the components of the whole system, including the inputs and the process used to produce the end-product. Second, there is an analysis of how the connectivity, cognitive ability and imperceptibility of the smart system can create specific risks. For instance, connectivity means that data inputs may be corrupted, incomplete, or misleading; that processing algorithms may be chosen because of the need for compatibility rather than its performance; and that poor quality outputs spread broadly and quickly, increasing the scope and likelihood of mistakes.[10]

3.3.　　Push and pull mechanisms should be used to ensure that firms conduct a thorough assessment of the value destruction potential of the technologies that they develop. Push mechanisms include the development of relevant guidelines and creation of audit and enforcement mechanisms. In turn, pull mechanisms include the investment in resources to identify and handle those risks (e.g., education; diverse workforce), as well as behavioural changes (e.g., through certification).[11]

4. What are the key short- and long-term risks and threats, and how can we ensure the devices, systems and networks of individuals, businesses and organisations are digitally-literate and cyber secure?

4.1.　　Technological advancement created issues around information security and various short-term cyber risk such as cyber-bullying, cyber-dating violence and hacking which, in the long-term, lead to mental health risk such as depression, anxiety, psychological distress as a key social concern in digital society[12].

4.2.　　Data from smart devices are an important and valuable asset. However, unlike other assets (e.g., people or capital), data ownership creates data network effects (DNE) for the platform owner. That is, the more user data accumulated by the platform owner, the more valuable the platform becomes to each user[13] . Therefore, DNE may result in *de facto* monopolies for smart device manufacturer, as a long-term risk.

4.3.　　One way to develop relevant awareness and behaviour, for safer use of technology, is through the use of quasi-simulations[14], whereby participants are required to assess an uncertain environment, plan and execute their actions; and obtain feedback through the use of metrics[15].

---

[10] Canhoto, A. I. & Clear, F. (2020). Artificial Intelligence and Machine Learning as business tools: factors influencing value creation and value destruction. Business Horizons, 63(1) DOI: https://doi.org/10.1016/j.bushor.2019.11.003

[11] Idem

[12] Paat, Y. F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, *19*(1), 18-40.

[13] Gregory, R. W., Henfridsson, O., Kaganer, E. and Kyriakou, H. (2021) *The role of artificial intelligence and data network effect for creating user value.* Academy of Management Review, 46 (3). pp. 534-551.doi:10.5465/amr.2019.0178

[14] Canhoto, A. I., & Murphy, J. (2016). Learning from simulation design to develop better experiential learning initiatives – An integrative approach. Journal of Marketing Education, 38(2), 98-106. DOI: 10.1177/0273475316643746

5. **How will current geopolitical concerns influence domestic consumers, e.g. regarding standards of imported goods or in how we can deal with cyber threats?**