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 than current systems?**

1.1. The main feature that distinguishes smart devices from any other devices that serve the same functional purpose (e.g., smart vs non-smart car) is the collection and transmission of data, over an internet connection. Smart technology can collect and transmit data about how they are used, and/or about their context of use, with little or no interference from users. Some devices can also interact with each other, with no human interference, and learn from each other (e.g., self-driving cars).

1.2. Accordingly, the most important impact of smart technology has been the datafication of daily life - i.e., the collection of data about most human and non-human (e.g., performance of machinery) activities, sometimes without the intervention - or even awareness - by those about whom data are being collected.

1.3. At the individual level, access to a continuous flow of granular and timely data fuels a desire to optimise performance (e.g., health and fitness) and productivity. But also exposes individuals to privacy risks[1].

1.4. In the workplace, datafication enables evidence informed decision making (e.g., pre-emptive maintenance, or designing workers' shifts); and creates opportunities for innovation[2]. However, it also changes the number and nature of jobs, and is leading to professional alienation[3]

1.5. In our towns and cities, datafication can support the achievement of SDGs, such as enhancing the environment by expending the circular economy[4]. However, that comes with the risk of uncontested surveillance[5].

---

[1] Brodie, C., Karat, C. M., Karat, J., & Feng, J. (2005). Usable security and privacy: a case study of developing privacy management tools. In *Proceedings of the 2005 symposium on Usable privacy and security* (pp. 35-43).

[2] Tabaghdehi, A. (2022) 'COVID-19 and Digital Economy: The Journey Towards a Digital Transformation in New Normal: How to Prepare for the Future', in *The Economics of COVID-19.* Emerald Publishing Limited. , 296. pp. 95 - 104. ISBN 10: 180071694X. ISBN 13: 9781800716940.

[3] Braganza, A., Chen, W., Canhoto, A. I. & Sap, S. (2021). Productive Employment and Decent Work: The Impact of AI Adoption on Psychological Contracts, Job Engagement and Employee Trust. *Journal of Business Research*. 131, 485-494. DOI: https://doi.org/10.1016/j.jbusres.2020.08.018

[4] Fernandes, K. Chaudhuri, A. & Kakar, A., (2022) Blueprint for Smart Cities: A Social Contract. A report published by citiesabc.com pp 1-71

[5] Mascheroni, G. (2020). Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology*, *68*(6), 798–813. https://doi.org/10.1177/0011392118807534

2. **Are there any groups in society who may particularly benefit from or be vulnerable to the increasing prevalence of smart technology, such as young or elderly people, people with disabilities and people likely to be digitally excluded?**

2.1. We start from the assumption that any citizen may, in principle, be able to benefit from smart technology, and, thus, focus our attention on those attributes that may cause vulnerability.

2.2. While some groups are at an increased risk of finding themselves in a vulnerable position (as per the list of protected characteristics already embedded in legislation[6]), it is the context rather than personal characteristics that determines vulnerability[7]. For instance, a pensioner's vulnerability to online scams arises from their unfamiliarity with new technology, not their age.

2.3. In terms of smart technology, vulnerability can result from:

a. Unavailability of technology, including:
   i. Hardware – e.g., assistive technology
   ii. Software – e.g., lack of features, lack of compatibility...
   iii. Internet connection – e.g., rural areas

b. Inability to use the technology, due to:
   i. Insufficient purchasing power – e.g., limited disposable income
   ii. Incompatibility with legacy technologies – e.g., old operating system in mobile phone
   iii. Digital skills – e.g., unaware that technology exists, or lack of perception of gaps[8]
   iv. Lack of representation in dataset – e.g., particular accents

c. Consequences of using the technology, including:
   i. Digital footprints – e.g., not understanding risks of mismanagement of digital footprint
   ii. Scams and frauds – e.g., hacking

2.4. Those citizens that find themselves at the intersection of two or more of the factors mentioned in 2.3 are at an increased risk of vulnerability.

3. **How can we incentivise or encourage design that is safe, secure, environmentally- and user-friendly and human rights compliant?**

3.1. The typical mechanism for ensuring compliance is through the imposition of standards. An example is the European Commission's ruling that all mobile devices on sale in the EU market will have to include a USB-C charging port, to reduce electronic waste and protect consumers[9]. However, standards and rulings focus on the end-product and, thus, are designed and

---

[6] Equality Act 2010

[7] Canhoto, A. I. & Dibb, S. (2016). Unpacking the interplay between organisational factors and the economic environment in the creation of consumer vulnerability. *Journal of Marketing Management*, 32(3-4), 335-356. DOI: 10.1080/0267257X.2015.1123759

[8] Stuart, R., Braganza, A., Charteris, V., & Jones, M. (2022) Digital Poverty in Margate: A Study of Two Hyperlocal Communities. A report prepared by Brunel University London and funded by The British Academy. pp 35.

[9] https://www.europarl.europa.eu/news/en/press-room/20220603IPR32196/deal-on-common-charger-reducing-hassle-for-consumers-and-curbing-e-waste [last accessed 14 June 2022]

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?**

5.1. There is no evidence to support the expectation that consumers would choose a brand because of their socio-political stance. For instance, customers' opinions on Brexit (from either side of the debate) do not influence purchase intention towards brands that moved production to the UK. However, their perceptions of such brands improved when the onshoring decision was deemed to improve the local economy or reduce carbon footprint[16]. That is, preference for domestic firms may be influenced by emphasising their corporate social responsibility initiatives.

5.2. Preference may also be influenced by raising the cost of non-domestic options (e.g., through taxation), or its performance risk (e.g., through sanctions). For example, President Trump's blacklisting of Huawei, in 2019, led to a decline of 47% in revenues in the consumer electronics part of the business (though the company recorded growth in other segments)[17].

---

[15] McIlwraith, A. (2021). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.

[16] Dey, B.L., Alwi, S.F., Babu, M.M., Roy, S.K. and Muhammad, S.S. (forthcoming), "Brexit or Brand it? The effects of attitude towards Brexit and reshored brands on consumer purchase intention", British Journal of Management

[17] Kynge, J. (2021). "Huawei suffers biggest-ever decline in revenue after US blacklisting", Financial Times, https://www.ft.com/content/dc170be7-262e-4616-9ef9-2a49c611c26b [last accessed 14 June 2022]