Written evidence submitted by Dr Lulu P. Shi, Prof Ekaterina Hertog, and Prof Victoria Nash

About

The Oxford Internet Institute (OII) – founded in 2001 - is a multidisciplinary research and teaching department of the University of Oxford, dedicated to the social science of the Internet. Our faculty are drawn from across the social sciences, humanities and data science, conducting rigorous, policy-relevant research into the societal implications of digital technologies, including smart technologies such as those which are the subject of this Enquiry.

This submission is authored by three researchers at the OII with a particular expertise in the ways smart technologies influence our everyday lives:
Professor Victoria Nash, a policy researcher and Director of the OII, focusing on Internet regulation and platform governance, with a particular interest in policy measures targeting children's online experiences;
Dr Lulu Shi, a sociologist focusing on the intersection between technology and society from a political economy perspective. She leads a project on education technology and its social impact;
Professor Ekaterina Hertog, a sociologist, whose research interests lie at the intersection of digital sociology and family sociology. She leads the ESRC-funded DomesticAI project that scopes the potential of digital technologies to transform domestic labor.

There are many aspects of OII research with relevance to this Call for Evidence, and we would be happy to provide further details of specific projects or provide introductions to other colleagues. In this submission we have chosen to focus on the balance between risks and opportunities provided by new smart technologies, as much of our research over the past 21 years has highlighted that both are usually associated with the rollout of new digital technologies, and that risks and resulting harms are often experienced by the most vulnerable or marginalized users.

Summary

In our submission we provide some examples of the risks associated with greater connectivity, such as the expansion of data collection, the complexity of managing smart devices, security risks and the impacts of opaque algorithmic decision-making. We stress the importance of careful consideration of the benefits of greater connectivity against such potential costs, and the importance of purposeful and reflective design and regulation to safeguard against the associated risks.

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?

The integration of smart and connected technologies into different aspects of our lives offers a wide range of potential benefits, promising to inform individual and public decision-making with finely grained real-time data, and offering direct interface with Internet services such as shopping, music and search. But these technologies bring risks as well as opportunities and may reinforce digital and social inequality. As such, the increased prevalence of smart technologies comes with no guarantee of improvement on the preceding systems. Concerns about privacy, data protection and exploitation abound, whilst high-profile data leaks and hacks have occurred even in sectors such as connected toys (e.g. VTech's data hack[1]), and baby monitors[2] where enhanced security protections might be expected. Connecting our lives across spheres inevitably means a huge amount of potentially sensitive data is collected about individuals. This data is utilized to make increasingly precise predictions about the most private matters, like pregnancy status.

As this information is collected by profit-maximizing organizations the data and the predictions based on it may be used in ways detrimental to individuals or in decisions which are opaque to them[3]. Further, some of the aspects of smart technologies that offer the most obvious benefits, do come at a cost. The ability of devices such as smart meters, home assistants, connected toys or activity trackers to operate without complex instructions via simple interfaces (i.e. without a computer screen) means that they are also less visible, their connectivity and data extraction hidden from their users[4].

There is insufficient space here to detail the full range of risks and opportunities associated with all these technologies, but the example of smart educational technology[5] in schools demonstrates some of the key issues.

Technology is used increasingly in educational settings and has brought about improvement in many areas, including enabling the continuation of education for students via remote schooling during the pandemic. The costs and risks of smart and connected technologies becoming increasingly prevalent in educational settings have received limited attention, but the current drawbacks are substantial:

---

[1] https://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children
[2] https://www.bbc.co.uk/news/technology-56141093
[3] Sadowski, J. (2019) When data is capital: Datafication, accumulation, and extraction. Big Data & Society.
[4] Van Deursen, A.J.A.M. & Mossberger, K. (2018) Any Thing for Anyone? A New Digital Divide in Internet-of-Things Skills. Policy and Internet. 10:2.
[5] Dr Lulu Shi's project specifically investigates socio-economic impacts of education technology.

a) *Designed by people without pedagogical training*: Most technologies for educational use are developed and advocated by tech companies rather than by the actual users, such as school teachers. Designers and producers of education technology often have engineering backgrounds and do not necessarily have expertise in pedagogy and teaching experience. Yet, when technologies fail to deliver what they promise, it is often teachers who are blamed as holding outdated attitudes and being resistant to technological innovations. Academic studies have pointed out the importance of focussing on technology producers[6].

b) *Designed to maximize profits not learning*: EdTech companies, like most other tech companies, are profit-maximizing entities. They present their products to investors promising lucrative return of investment (ROI), and the actual users – teachers and students, are of second priority. As a result, the future of education is shaped by investors in education technology who create narratives that maximize the ROI[7]. Schools such as AltSchool and XQ Super School are examples of Silicon Valley founded schools that collapsed when investors' interests dropped and profit fell[8]. The issue is that private firms are businesses, and their priorities may be in line with public interests, but they can change flexibly, as they often do[9].

c) *Collection of personal data with no real option to opt out*: It is a common practise for the big tech companies, including edtech companies, to package private data collection with obscure language and terminologies that are difficult for the average person to understand. As a result, users often do not have a clear understanding about the terms and conditions they sign up for and what that means for their personal data. As a study on Google has shown, users of Google Apps for Education (GAFE) are misled when they presume that Google is a 'free service', which is in fact based on and profits from users' behavioral data[10]

---

[6] E.g. Manolev, J., Sullivan, A., & Slee, R. (2019) The datafication of discipline: ClassDojo, surveillance and a performative classroom culture, Learning, Media and Technology, 44:1, 36–51, DOI: 10.1080/17439884.2018.1558237

[7] E.g. Williamson, B. & Komljenovic, J. (2022) Investing in imagined digital futures: the techno-financial 'futuring' of edtech investors in higher education, Critical Studies in Education, DOI: 10.1080/17508487.2022.2081587 and Komljenovic, J. (2022) The future of value in digitalised higher education: why data privacy should not be our biggest concern. High Educ 83**,** 119–135. https://doi.org/10.1007/s10734-020-00639-7

[8] Williamson, Ben. (2017a) Big Data in Education: The Digital Future of Learning, Policy and Practice. 1 Oliver's Yard, 55 City Road London EC1Y 1SP: SAGE Publications Ltd.

[9] Greene, P. (2016) What Can We Learn From An Experimental High Tech Wunderschool Failure?, Forbes. https://www.forbes.com/sites/petergreene/2019/07/15/what-can-we-learn-from-an-experimental-high-tech-charter-wunderschool-failure/

[10] Lindh M, Nolin J. (2016) Information We Collect: Surveillance and Privacy in the Implementation of

. In many cases, it is organizations that purchase the licenses of tech products on behalf of the employees and students, and there are few or no alternatives for the users, who have little choice but to agree with the terms and conditions.

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?

Well designed and inclusively-developed technologies could certainly bring valuable benefits to marginalized groups, for example with smart meters potentially reducing energy costs in the home, or fitness trackers empowering individuals to monitor their own health, potentially in conjunction with health services. In developing countries access to mobile phones has been associated with lower gender inequalities, enhanced contraceptive use and lower maternal and child mortality[11]. Adopting smart domestic technologies can reduce time currently spent on unpaid domestic work and reduce gender inequalities at home in both developed and potentially developing world[12].

But the risks posed to more vulnerable individuals must also be taken into account, and research suggests that the digital divide matters as much in relation to smart technologies as it has to other forms of Internet use. For example, smart devices might not demand the communicative skills of social media, but data literacy is key to non-exploitative use. Ensuring secure and privacy-protecting use requires sophisticated understanding of device and network settings, which research has shown is less likely to be manifested in those with the lowest levels of education[13], and which is also relevant when considering the challenges for elderly adults or child users. Research into children's understanding of online privacy risks, for example, has shown that they have a better understanding of interpersonal risks (e.g. sharing too much or sensitive personal information with someone and then regretting it) than they do of other types of data risk such as data breaches or future reputational damage[14]. In the context of smart devices,

---

Google Apps for Education. European Educational Research Journal, 15:6, 644–663. DOI:10.1177/1474904116654917

[11] Rotondi, V., Kashyap, R., Pesando, L. M., Spinelli, S., & Billari, F. C. (2020) Leveraging mobile phones to attain sustainable development. Proceedings of the National Academy of Sciences, 117(24), 13413-13420. doi:10.1073/pnas.1909326117

[12] Hertog, E., Fukuda, S., Matsukura, R., Nagase, N., & Lehdonvirta, V. (2022, February 9) The future of unpaid work: Estimating the effects of automation on time spent on housework and care work in Japan and the UK. https://doi.org/10.31235/osf.io/swe7n

[13] Van Deursen & Mossberger (2018) Any Thing for Anyone? A New Digital Divide in Internet-of-Things Skills. Policy and Internet. https://doi.org/10.1002/poi3.171, 10; 2, 122-140.

[14] Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in

this might suggest that children would under-estimate the risks involved from collection of sensitive data such as health data, or content such as photographs, even when significant data hacks or leaks have occurred.

Our own research also shows that the way people imagine “the future of” technologies is socially contingent, influenced by the experts’ lived experiences meaning that different social groups will have different expectations of technology which may limit the potential benefits available to them[15]. Ensuring diverse groups of experts are involved in designing connected technologies is a crucial step towards balancing the benefits and risks of smart technologies across all social groups.

A further concern is that these smart technology resources will be deployed in stretched public services to make cost savings, meaning the most vulnerable may be forced to use these tools, but not for their own benefit. For example, some classroom technologies have surveillance functions that can flag up deviating students’ behaviors and notify the teachers. These functions are often portrayed as an efficient and effective tool to alleviate overcrowded classrooms, where teachers have limited capacity to devote attention to each individual student. Yet surveillance technologies are based on intensive and extensive data collection, which may stand in odds with student safeguarding and privacy. Large classes and poor student-to-teacher ratios are more common in poor schools and in deprived areas, while well-resourced schools can afford more teachers and more teacher-time per student. This leads to poorer schools being more likely to adapt and rely on data-collecting surveillance technologies, and students from poorer area potentially being more intensively tracked throughout their education[16]. In other public service areas, such as policing and health care, it is well-documented how surveillance and predictive technologies disproportionately affect the most powerless and marginalized people[17].

Finally, it is also worth noting that data gathered by smart devices such as surveillance tools in EdTech platforms or smart assistants in the home might itself be used in algorithmic decision-making in ways that could negatively affect the wellbeing of some users, especially vulnerable ones. For example, the same

---

a digital age. Research findings. London: London School of Economics and Political Science

[15] Lehdonvirta, V., Shi, L., Hertog, E., Nagase, N., & Ohta, Y. (2022) The future (s) of unpaid work: How susceptible do experts from different backgrounds think the domestic sphere is to automation. https://doi.org/10.31235/osf.io/vzwyd

[16] Knox, J., Williamson , B. & Bayne, S. (2020) Machine behaviourism: future visions of ‘learnification’ and ‘datafication’ across humans and digital technologies, Learning, Media and Technology, 45:1, 31-45, DOI: 10.1080/17439884.2019.1623251

[17] Eubanks, V. (2018) *Automating Inequality*. New York: Macmillan.

algorithmic processes that sometimes serve up ever more extreme content on social media processes may result in similarly problematic content being delivered over smart speakers, whilst children with poor behaviour could conceivably find their educational options restricted rather than expanded through ill-designed software. The use of unregulated 'babytech' such as smart socks and cot sensors also raises concerns about the risks of decisions made about infant health and wellbeing on the basis of unreliable technologies[18]. It will also be important to initiate a wider societal conversation about the appropriate place of algorithmic decision-making in sensitive contexts such as education, parenting or social care, and in particular to discuss whether we are comfortable with scenarios where smart devices inform key decisions about individuals on the basis of data points rather than situated knowledge of the person as a whole.

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

Consumers adopt and continue to use technologies even when they perceive them as untrustworthy. Fetterolf and Hertog find that most of the young college-educated American Amazon Alexa users distrusted Amazon as a company and were concerned about its surveillance practices. Their response was to minimize their discomfort and resign themselves to the situation or to mentally separate Alexa from Amazon and continue using it [19]. This response is often encouraged and facilitated by companies behind the smart connected devices which are often very secretive about how they collect and how they use customer data and which also often humanize their devices. Marginalized groups, such as less educated or lower-income individuals, may be particularly unable to act upon any concerns they have about adopting new smart technologies. They do also commonly give up personal privacy in order to secure cheaper digital consumer products. The reality of consumer acceptance of new smart digital technologies despite worries about associated risks, suggests that additional worries, such as geopolitical concerns, may not influence individual decisions in the absence of additional incentives, such as banning certain foreign companies or goods making undesirable technologies difficult or impossible to use.

In the long term, regulating big tech companies to mandate practices that return as much control over personal data back to individuals, enabling some level of

[18] Nash, V., Davies, H. & Mishkin, A. (2019) Digital Safety in the Era of Connected Cots and Talking Teddies. Available at SSRN: https://ssrn.com/abstract=3407264

[19] Fetterolf, E., & Hertog, E. (2022) It's Not Her Fault: Trust through Anthropomorphism among Young Adult Amazon Alexa Users. https://doi.org/10.31235/osf.io/bkx3n

personal control and educating consumers to make active choices when using smart connected technologies may help to address the root cause of digital resignation.

4) Do existing frameworks, like data protection legislation and the Public Security and Telecommunications Infrastructure Bill, adequately address concerns with smart technology, and if not, how could they be changed?

Existing legislation and regulation increasingly provides a strong foundation for addressing concerns with smart technology, but many gaps still persist. Internet of Things security weaknesses such as inclusion of default passwords, and failures to allow for automatic security updates, continue to be a significant concern, affecting both consumers and businesses in large numbers[20]. In this light, the recent announcement in the Queen's Speech that the Product Security and Telecommunications Infrastructure Bill will now proceed through Parliament this year is very welcome, although debate continues as to whether the proposed measures will prove sufficient to prevent the worst security flaws. Much will also depend on the extent to which the resulting law is enforced, and we would highlight that existing consumer protection frameworks seem inadequate to the task, not least given consumers' current reliance on local trading standards bodies for recourse.

It is notable that at the European level, it has been non-governmental organizations rather than public bodies who have done the most to highlight the most egregious security flaws of connected devices such as the My Friend Cayla doll, deemed an 'illegal transmitting device' by the German government [21]. This is certainly an area where the UK government could do more to work with consumer rights organizations such as Which or Citizens Advice Bureaus, which have the advantage of being well-trusted by citizens. The availability of imported and discounted goods from online retailers also continues to provide a challenge to UK consumer protection, particularly as those on lower incomes have little option but to look for the lowest prices.

Data protection and privacy rights must also be prioritized, particularly for children and vulnerable users. The use of smart technologies in workplaces or public services such as education merits special attention here, as it is unclear that existing legal protections are being effectively applied with some evidence of

[20] https://www.which.co.uk/news/article/smart-products-from-the-biggest-tech-brands-easily-hacked-in-which-tests-az2Ne3k7FXT1

[21] https://www.bbc.co.uk/news/world-europe-39002142

governance gaps which must be addressed[22]. In order to ensure that UK users are able to enjoy the benefits of smart and connected devices in the future, it will be vital to ensure that data protection provisions are not significantly weakened when Parliament considers the Data Reform Bill later this year.

We would be delighted to discuss these ideas in greater detail as the Committee advances its inquiry.

[22] Digital Futures Commission (2021) Governance of Data for Children's Data in UK State Schools. Available at: https://digitalfuturescommission.org.uk/wp-content/uploads/2021/06/Governance-of-data-for-children-learning.pdf