Response to Call for Evidence

Digital, Culture, Media and Sport Committee:

Connected tech: smart or sinister?

Submitted by

Professor Derek McAuley, Professor Andy Crabtree and, Dr Anna-Maria Piskopani **(**University of Nottingham); Dr Jiahong Chen (University of Sheffield); Dr Lachlan Urquhart (University of Edinburgh)

23 June 2022

Introduction

1. Horizon is a Research Institute centred at the University of Nottingham and a Research Hub within the UKRI Digital Economy programme. 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. Professor Derek McAuley is Director of Horizon and Deputy Director of the UKRI Trustworthy Autonomous Systems Hub. Professor Andy Crabtree is Professor of Computer Science at University of Nottingham. Dr Lachlan Urquhart is Senior Lecturer in Technology Law at Edinburgh Law School, and Co-Investigator of the UKRI Trustworthy Autonomous Systems Node in Governance and Regulation. Dr Jiahong Chen is Lecturer in Law at Sheffield Law School. Dr Anna-Maria Piskopani is a Research Fellow at the Horizon Digital Economy Research Institute.
2. This submission aims to address a selection of questions formulated in the Committee's *Call for Evidence* by presenting findings and views based primarily on research undertaken by us, although we have also drawn on publicly available sources where appropriate. We will focus on certain case studies and areas of technology industry with a view to informing the Committee's inquiry. We would be happy to be contacted for further evidence and for this submission to be published in full.

Question 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?

3. Smart technology based on the Internet of Things (IoT) promises to improve security and energy-efficiency in homes and workplaces (by automatically controlling lighting, heating and cooling and with precise delivery when and where it is needed), public services (innovative public procurement), and to generally raise the quality of life for inhabitants of towns and cities by optimizing city functions—from more efficient use of utilities and other services to reducing traffic congestion and pollution.
4. Concurrently, these technologies in people's lives create an omnipresence of surveillance. There are different privacy challenges arising from constant networked sensing, for example, in using smart devices in private homes, in workplaces where spaces can be private, semi-private and semi-public, in public buildings that can also be workplaces, and in the open air in city/town streets.

5. In addition, IoT devices pose challenges when connected to the cloud. IoT refers to the network of cyber-physical objects that contain, for example, software and sensors that allow 'things' to be connected to the Internet and each other. These connected 'things' can interact and exchange data, including personal and even sensitive data, whilst being remotely controlled or automated. IoT solutions can involve cloud services and artificial intelligence (AI). This means there is an IoT spectrum spanning devices that can be smart without needing to be connected to a cloud service, others that in order to be smart must be connected to a cloud service, and dumb connected devices that simply provide information and access to a smart cloud service.

6. However, it is possible in the domestic environment to develop a home network-attached computer that collates data from IoT devices deployed in the home and to make data implicating users and their behaviour available to downloaded apps to deliver personalised services while constraining the onward flow of data (e.g., our work on Databox). Databox enables 'data minimisation', meaning that the raw data stays on-the-box under users' control and that very little data (only the results of data processing on-the-box) is shared with third-parties, if anything is shared at all. The data thus remain in a personal Databox, safe and secure, allowing users to see and control exactly how data are processed and to make informed choices of concerning the uses of their data by third-parties[1].

7. Today a similar effort is being attempted by industry. There is a new smart home standard emerging called *Matter*, which provides a unified protocol that seeks to enable smart home devices from all vendors to co-exist, communicate, and be controlled using the local home network rather than via the cloud while also providing a common means of provisioning (i.e. add new devices)[2].

8. Smart devices that are less reliant on cloud services can be both more resilient and privacy-preserving than those that require a cloud service. In enterprise networking resilience to component failure is commonly achieved via redundancy, whereas in the domestic environment the broadband connection is a single point of failure. Hence, smart home devices that are not reliant on continuous internet connectivity for operation provide greater resilience and can be more 'user friendly'. Likewise, for some smart devices we need to protect against power outage – indeed smart intruder and smoke alarms that rely on power and cloud-based services to raise an alarm condition are not very useful – and, indeed, do not comply with established British Standards[3].

9. Another example is smart energy meters. These are considered better than a conventional meter because they can provide more information about energy consumption, enable automated meter reading instead of manual reading, and transfer readings at regular intervals. Smart meters can also be connected to smart home devices, such as energy monitors, to enable the tracking of individual appliances, to improve control and save energy. Smart meters have been increasingly used in the UK with the stated intent to help households reduce the cost of gas and electricity by monitoring their usage in real time. However, it has recently been reported that millions of smart meters started to malfunction due to the "unreliable signal"[4]. As their users could not know their readings, they could not benefit from their "smartness". Other users pointed out that using smart meters had no impact on their energy usage. Consequently, while smart meters promise many social and personal benefits, they often frustrate consumers, while the underpinning pervasive collection, retention, and use of personal data without consumer benefit, only serves to undermine trust in these "smart" systems.

[1] https://www.horizon.ac.uk/project/databox/
[2] https://csa-iot.org/all-solutions/matter/
[3] British Standard, BS 5839, BS 8243
[4] https://www.theguardian.com/money/2022/jun/04/why-are-so-many-smart-meters-turning-dumb-greatbritain

Question 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?

10. It is often proposed that smart technology will particularly help older people and those living with disabilities. This includes smartphones, smart security technologies, and digital home assistants being used to improve or maintain their ability to perform important everyday activities and feel secure in their own homes. However, there are considerable barriers to such use: smart devices have confusing instructions, often require difficult setup procedures, are expensive and lead to privacy concerns[5]. They also pose challenges around managing third party access to data, such as caregivers or family, and how negotiation around access can be provided in ways that enable dignity and autonomy for vulnerable users[6].

11. Smart technology has data security risks, especially where it is used for behavioural profiling with vulnerable people. According to the ICO "individuals can be vulnerable where circumstances may restrict their ability to freely consent or to object to the processing of their personal data, or to understand its implications"[7]. Privacy policies are hardly understandable by the general public and even more difficult for vulnerable people such as younger or older people or people with mental disabilities. Privacy policies for children are especially confusing, difficult to comprehend, often long and complex, and while often it states a requirement for guardians' consent, it is not always actually required or checked. For younger users, further research is needed around how to implement the UK's Information Commissioner's Office (ICO) Age Appropriate Design Code of Conduct to ensure their interactions with IoT devices occur in data protection compliant ways.

12. In addition, the increasing prevalence of smart technology falsely leads to the assumption that access to these systems is ubiquitous in society. For example, the two-factor authentication that has been introduced to increase security in banking and taxation requires that customers, including elderly and those in socio-economic deprivation, have the digital infrastructure, devices and know-how to participate. We should not assume that a 'one size fits all' model works, but be sensitive to the many and varied circumstances that can affect digital inclusion and participation; not just vulnerability but location, income, age, education, etc.

13. If suppliers rigorously implement the data protection by design and default (DPbDD) principle (DPA 2018 / GDPR), they will demonstrate how to provide privacy-friendly smart technology to everyone by default and hence ensure vulnerable users are included[8]. Well-established companies, whose paradigm small and medium enterprises follow, should be the ones to lead this shift to rigorous DPbDD and change industry practices to better support users.

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

14. Smart technology applies in different domains and is therefore regulated by different frameworks and rules. However, smart devices often do not comply with existing regulatory frameworks e.g., data protection, product safety. There has been progress establishing stronger rules for IoT security

[5] https://doi.org/10.3389/fcomp.2022.835927

[6] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf; https://doi.org/10.1093/idpl/ipac001

[7] Information Commissioner's Office, 'When Do We Need to Do a DPIA?' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-tothe- general-data-protection-regulation-gdpr/data-protection-impactassessments-dpias/when-do-we-need-to-do-a-dpia/> accessed 6 October 2021. 9 Art 29

[8] https://doi.org/10.1093/idpl/ipac001

through the proposed UK Product Security & Telecoms Infrastructure Bill e.g., on issues of default passwords and making consumers aware about software update timelines. A first step should be enforcement of existing laws and standards, such as British Standards for smoke alarms and intruder alarms that have already been mentioned.

15. In addition, even though smart technology promises to be environmentally friendly, sustainability of devices is impacted by the unstable, rapidly changing industry with expensive smart devices becoming useless when a company stops providing updates or providing a necessary cloud service. Improving repairability and modularity of these devices, to guard against unnecessary eWaste and support a more circular economy for the IoT, is key.[9]

16. Engaging the public about the potential risks and harms of smart AI technologies alongside their anticipated benefits is key to fostering more responsible industry priorities.

17. It is also important that industry is prepared for new regulations, such as the forthcoming EU AI Act. Regulation will attempt to minimise the potential harms of smart technologies (e.g., consumer profiling, behaviour preferences etc.)[10]. Supporting UK industry through regulatory sandpits and guidance such as the Code of Practice for Consumer IoT Security[11], for example, will help develop devices that comply with the new regulations. This would have financial benefits, enabling UK industry to get smart technologies to EU and international markets with speed and without burdens or delays. Such steps will enhance the reputation and competitiveness of British smart products in the global market.

18. In our research we have identified a number of technical, organisational and legal barriers to developing safe, secure, environmentally- and user-friendly smart home products. We have made a number of recommendations, including adopting a human-centred approach to IoT security in smart homes; ensuring vendors implement technical and organisational safeguards that support the growing role of domestic data controllers in managing data processing in the smart home; expanding the scope of cybersecurity laws to forecast and manage risks across the lifecycle of IoT devices; rolling out certification and labelling schemes that increase consumer trust in devices; and promoting the need for security across the IoT supply chain[12].

Question 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?

19. There is evidence backed concern that smart devices can lead to tracking the everyday lives of people in their own homes and workplaces by building detailed profiles of all individuals based on their domestic and work activities. Those profiles are enriched with personal data drawn from other online and offline sources and can allow aspects of an individual's personality or behaviour, interests

[9] https://www.law.ed.ac.uk/news-events/news/ps12m-project-fixing-future-right-repair-and-equal-iot-funded-uk-epsrc

[10] https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/the-benefits-and-harms-of-algorithms-a-shared-perspective-from-the-four-digital-regulators

[11] DCMS, 'Code of Practice for Consumer IoT Security' (2018) https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[12] https://www.tandfonline.com/doi/full/10.1080/13600834.2021.1957193

and habits to be determined, analysed and predicted and can be used for marketing or advertising purposes, data-brokering and employee performance monitoring.

20. Profiling and automated decision-making techniques can pose significant short and long-term risks for individuals' rights and freedoms. Profiling can perpetuate existing stereotypes and social segregation, particularly as individuals might not know that they are being profiled or understand what is involved with these opaque processes. In some cases, profiling can lead to inaccurate predictions, denial of access to public services and unjustified discrimination[13].

21. Smart cities have deployed surveillance technologies powered by automatic data mining, facial recognition, and other forms of artificial intelligence. Some of them are approaching the precipice of a hyperconnected 'internet of everything', which comes with unprecedented levels of risk tied to billions of unsecured devices. As cities become ever more connected, the risks of digital harm by malign actors grow exponentially. They can be targeted for data theft, system breaches, and cyberattacks, all of which can undermine their operation and provision of essential services[14]. Securitisation of public space with smart video devices in private, semi-private and public spaces also impacts human rights, data protection and equality rights[15]. Human rights impact assessments may help anticipate the range of risks and strategies to mitigate these.

22. There are research projects and industry efforts with the new smart home standard called *Matter* as well as the *Zigbee* alliance to develop smart devices that do not need to be connected to the cloud and provide alternative privacy-preserving solutions[16]. These initiatives should be promoted, considered as best practice and supported.

23. In addition, edge-based personal information management systems such as the Databox can integrate with a wider class of privacy-preserving solutions to help users determine how their data is used and increase local control over who has access to it. This shift to 'small data' led systems can empower users and address data protection compliance concerns, particularly around opacity of data flows and power asymmetries involved in personal data processing[17].

Question 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?

24. As mentioned above, a hyperconnected 'internet of everything' comes with unprecedented levels of risk tied to vast numbers of unsecured devices and cyber threats. Authorities, companies and individuals need to build digital security into all domains of governance, infrastructure, commerce, and everyday life. We should mandate and enforce standards that require all internet-enabled devices sold and deployed in the UK, imported and locally manufactured, have minimum password protection, authentication, and encryption built-in.

---

[13] https://ec.europa.eu/newsroom/article29/items/612053/en

[14] https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g

[15] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

[16] https://csa-iot.org/all-solutions/zigbee/

[17] Urquhart, Lachlan and Chen, Jiahong, On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity (June 17, 2020). Crabtree, A. Mortier, R. Haddadi, H. Privacy by Design for the Internet of Things: Building Accountability and Security. IET Press Forthcoming, Available at SSRN: https://ssrn.com/abstract=3629119

25. As we have highlighted in previous submissions, additional technical and organisational measures should be taken by smart devices vendors in accordance with UK GDPR to boost consumer confidence[18]. Technical measures enabling data protection by design and default (e.g., data minimisation, purpose limitation, use of anonymization/pseudonymization, and end-to-end encryption) and organisational measures (e.g., data protection impact assessments, certification schemes, transparent data processing policies, internal compliance audits, and effective staff training), which together result in consumer products in which privacy and security are embedded by default.

26. Consumer education on IoT cybersecurity is essential. The wide variation in security quality means product labelling standards will be important because users cannot easily know how safe IoT devices are. The label system could also help make smart tech manufacturers accountable[19].

Question 6. 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?

27. The main legal safeguard addressing smart technology concerns is **data protection law; the DPA 2018 or UK GDPR.** The law introduces provisions to ensure that profiling and automated individual decision-making are not used in ways that have an unjustified impact on individuals' rights. There are specific transparency and fairness requirements, greater accountability obligations, specified legal bases for data processing, rights for individuals to oppose profiling and specifically profiling for marketing if certain conditions are met, and the need to carry out a data protection impact assessment[20]. Attempts to change the UK data protection landscape risks undermining the tools needed to ensure secure, safe and privacy preserving IoT. In particular, this includes removal of the accountability principle and data protection impact assessments.[21] Overall, shifts that the PSTI Bill seeks to establish in the IoT market are welcome, albeit ensuring responsiveness to and monitoring emerging security threats will be key.

28. As highlighted in our previous research and related submissions, guidelines and case law regarding joint controllership and controller/processor concepts have primarily focused on the business-to-business model. As we have pointed out, there is need to understand the differentiation of responsibilities between vendors and domestic users in the home, and how they can satisfy their respective obligations given the power imbalances between them[22].

29. Data protection legislation relies on the presumption that data protection by design and default will be implemented by data controllers and that consumers of smart devices will be aware of their rights and protect themselves from unreliable vendors and their obligations to respect other people's rights as neighbours, visitors etc. Enforcing data protection by design and default, and raising industry and public awareness, is of a major importance.

---

[18] https://doi.org/10.17639/hdyt-bd62

[19] https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons

[20] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). Article 29 Data Protection Working Body.

[21] https://doi.org/10.25878/gsc1-vz67

[22] https://doi.org/10.17639/H3HS-0E76, https://academic.oup.com/idpl/article/10/4/279/5900395

This submission was supported by the EPSRC Grant Number EP/T022493/1. Any enquiries regarding this submission should be sent to horizon@nottingham.ac.uk