Written evidence submitted by The UKRI Trustworthy Autonomous Systems Hub (TAS Hub), The UKRI Trustworthy Autonomous Systems Node in Resilience, The UKRI Trustworthy Autonomous Systems Node on Security, The UKRI Trustworthy Autonomous Systems Node on Verifiability

Connected tech: smart or sinister?

A call for evidence from Department for Digital, Culture, Media & Sport

Executive summary

Impact of increasingly prevalent smart technologies

We think that these changes will result in better or worse futures will be determined in large part by what is prioritised in technological innovation, and to what extent (if at all), previously marginalised, silenced, and exploited voices become part of the conversation. Our major concern is that innovation for profit is incentivised over societal benefits. We recommend that the government incentivises innovation for societal benefit**.**

Impact of smart technologies on different groups

- **Increased risks, especially for the most vulnerable and marginalised in society**

Smart technologies can improve the lives of vulnerable people but at the same time pose more significant risks if not appropriately managed. Therefore, we advocate for more inclusive development of smart devices at every stage of the product lifecycle (e.g. design, testing, implementation and maintenance). For example, datasets used for training, testing, and validating smart technologies are developed for common use cases; taking into account underprivileged and diverse parts of the society is key to their successful and fair adoption. While some technological solutions can be developed especially for vulnerable groups, a recent example with eye implants showed there is no protection once a company decides to end its production. We also advocate for more research with diverse groups. Smart technologies are mainly developed for commercial purposes, meaning that they do not consider different people's needs and appetite for adoption.

- **Digital literacies and skills**

The government needs to take responsibility for equipping society with the skills needed to use smart technologies in a safe and efficient way (eg to manage their privacy settings or set up secure passwords). Essential Digital Skills Report 2021 showed that c.10 million (19%) of UK adults do not have fundamental digital skills (for example, be able to use a device, connect to a Wi-Fi network and create and update passwords).

Working with smart technologies will require more advanced skills that typical interactions with banking and other governmental online services. Autonomous systems that act on behalf of humans will need to new skills to interact with so that the operation of human-machine systems can be deemed dependable.

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

- **User-centred research and design**

People are not aware of certain functions that are designed and developed to protect their privacy or ensure security. We advocate to incentivise and promote companies to conduct user-centred research to make sure that their products are used in a safe and secure way, while their users are aware of different functions.

- **Standardisation and more certifications of smart technologies to gain an understanding of their environmental impact**

The government, in order to achieve its climate goals, needs to give careful consideration and develop policies to ensure the sustainability of smart technologies during their whole product life cycle (production, manufacturing and disposal). Smart technologies also offer the opportunity to capture emissions data more accurately than previously possible.

The key short- and long-term risks and threats

- **Respecting an individual's autonomy.**

It is imperative that individual users maintain the ability to remain in control and manage the use of smart systems, influence and direct decision-making, and understand the role that such technologies play in their lives.

- **Privacy and data protection**

As the technology is largely data-driven, adherence to good data protection practices and the practice of good and lawful data stewardship is paramount. The use of cameras and monitors for tracking and surveillance purposes and used in many smart technology applications pose a risk of intrusion upon persons' privacy rights.

- **Behavioural manipulation.**

Smart technologies can threaten interests by using discriminatory, deceptive, and manipulative practices such as *nudging* and *dark patterns*.

- **Use of voice, facial, and emotional recognition systems.**

Voice, facial, and emotion recognition systems, used in smart technologies, may pose challenges to users' privacy, free expression, and social justice.

- **Cyberattacks and data breaches.**

Greater use of smart technologies demand hacking and cyber security protections. Poorly secured smart products and services threaten persons' online security, and subsequently, their privacy and safety.

- **Developing common mental models**

Without common mental models, stakeholders cannot find a common ground to operationalise and understand the nature of smart technology. This can lead to levels of consumer confusion.

- **Mixed initiative decision making and provenance tracking**

Without tracking the provenance of decisions in systems of humans and machines, we are likely to expose humans and organisations to ethical risks that they may not be responsible for nor equipped to deal with.

Concerns with smart technologies and existing regulatory frameworks

Regulatory and policy-development, guidance measures, and increased awareness and education can be used to overcome the concerns raised. These concerns can be managed and mitigated through an effective governance regime. Although there are existing frameworks and legislation applicable to smart technologies, they do not go far enough in addressing the unique risks posed by smart technologies. Gaps remain in the regulatory framework and policy is fragmented. We suggest that this requires urgent consideration.

About Authors

Professor Richard Hyde is Professor of Law, Regulation and Governance at the University of Nottingham. He is a Co-Investigator on the UKRI Trustworthy Autonomous Systems Hub. His research interest relates to law and technology, and particularly how new technologies affect consumers.

Dr Joseph Lindley, Dr Michael Stead and Professor Paul Coulton are part of Imagination Lancaster, Lancaster University's Design-led research lab. They lead and collaborate on a range of projects funded by the Trustworthy Autonomous System Hub, PETRAS National Centre of Excellence for IoT Cybersecurity, and the EPSRC's Equitable Digital Society initiative. Their work champions the use of Design Research in the context of socio-technological challenges, explores new and emerging approaches for human-centred computing, and addresses the sustainability challenges posed by 21st-century technologies.

Dr Justyna Lisinska is a social-technical researcher, specialising in how people impact technological development and how technology impacts people's lives with a particular interest in user-centred research. She is a Research Fellow based at King's College London, the Policy Institute, working on developing a policy programme for the Trustworthy Autonomous System Hub.

Dr Luke Moffat is a philosopher and researcher in the Sociology department. He designed cross-sector collaborations for the TAS Security Node at Lancaster University. He has experience producing original research in ethics of technology based on these collaborations, including the Disaster and Risk Management Domain.

Professor Mohammad Reza Mousavi is the principal investigator of the UKRI Trustworthy Autonomous Systems (TAS) Node on Verifiability. He is also a Professor of Software Engineering at the Department of Informatics (King's College London). Mohammad has extensive experience in and engagement with the connected and autonomous vehicles (CAVs) domain.

Professor Gopal Ramchurn is the director of the UKRI Trustworthy Autonomous Systems Hub and Professor of Artificial Intelligence. His work concerns the design and operation of human-machine teams.

Professor Paurav Shukla is a co-investigator on the UKRI Trustworthy Autonomous Systems (TAS) Hub programme. He is also a Professor of Marketing and Head of the Department for Digital & Data-Driven Marketing at the University of Southampton. He has led and been involved in several grants from ESRC, InnovateUK, and other international bodies, and published high-impact research.
Dr Beverley Townsend is a legal and ethics researcher at the York Law School, University of York. She works in the fields of resilient autonomous systems and robotics, law, ethics, artificial intelligence, and policy and regulatory development. Her background is in law, human rights, and technology. Bev is a part of the UKRI Trustworthy Autonomous Systems Node in Resilience working on projects to improve the socio-technical resilience and trustworthiness of autonomous systems.
Dr Jennifer Williams is a Research Fellow at the University of Southampton working on artificial intelligence and audio processing. Her work explores interdisciplinary approaches to smart building design, especially for services related to improving occupant comfort while also reducing resource consumption and energy costs. She is part of the UKRI Trustworthy Autonomous Systems Hub.

Citation

The UKRI Trustworthy Autonomous Systems Hub, The UKRI TAS Node in Resilience, The UKRI TAS Node on Security, The UKRI TAS Node on Verifiability (2022) *A Response to: Connected tech: smart or sinister?*. DOI: 10.18742/pub01-092

About

The UKRI Trustworthy Autonomous Systems Hub (TAS Hub) (EP/V00784X/1), assembles a team from the Universities of Southampton, Nottingham and King's College London. The Hub sits at the centre of the £33M Trustworthy Autonomous Systems Programme, funded by the UKRI Strategic Priorities Fund. The role of the TAS Hub is to coordinate and work with six research nodes to establish a collaborative platform for the UK to enable the development of socially beneficial autonomous systems that are both trustworthy in principle and trusted in practice.
The UKRI Trustworthy Autonomous Systems Node in Resilience (EP/V026747/1) The project brings together the disciplines of computer science, engineering, law, mathematics, philosophy and psychology from five UK universities to develop a comprehensive toolbox of principles, methods and systematic approaches for the engineering of resilient autonomous systems.
The UKRI Trustworthy Autonomous Systems Node on Security (EP/V026763/1) its research centred around a seamless collaboration between fundamental cross-disciplinary security research and autonomous systems research at Lancaster and Cranfield Universities**.**
The UKRI Trustworthy Autonomous Systems Node on Verifiability (EP/V026801/2), brings together a multi-disciplinary and diverse team of researchers with expertise in AI, robotics, human-computer interaction, systems and software engineering, and testing. Our goal is to develop a unifying framework that will integrate rigorous verification techniques for autonomous systems. Our framework will support the heterogeneous and adaptive nature of

verification techniques, their scale, and their levels of abstraction: from requirements and planning to coding and control algorithms to actual hardware and robotic implementation.

Some work is being presented as part of funded projects: Design Research Works - UKRI - MR/T019220/1, Experiencing the Future Mundane - EPSRC - EP/S02767X/1, Fixing the Future: The Right to Repair and Equal-IoT - EPSRC - EP/W024780/1, Cyber Security of the Internet of Things - EPSRC - EP/N023234/1.

Responses

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?

There is a huge amount of industrial innovation, government investment, and media attention being directed toward smart and connected technologies, their purported benefits, and associated challenges. Included in this attention is a widespread conception that smart technologies, particularly autonomous and AI-based technologies, have created an entirely new realm of technological experience. The recent media furore around a Google researcher claiming their AI chatbot is sentient speaks to this. (see Bogost, 2022). One challenge to establishing exactly how, for better or worse, smart and connected technologies will alter human life is an intense connection often made both by media and academia, that these technologies will ‘take over’ or ‘replace’ fundamental aspects of human life and experience. Common to all of these arguments, positive and critical, is the assumption that no matter what happens, these technologies are here to stay, and will only keep coming. Hidden in this assumption is in fact the belief that by existing, these kinds of technologies are automatically better than whatever preceded them. It is important while envisioning futures with smart and connected technologies, to combat misinformation and sensationalism, but also to be critical of *techno-solutionism*, in which problems created by technology can only be solved via technical means.

With this in mind, some likely significant changes across home, work and cities are:

- **Expansion of datafied life** - more data collected on more people shared between more parties
- **Everyday surveillance** - at work and at home, things previously deemed private/unimportant becomes objects of datafication
- **Potential widening of inequalities** - between those with access to new technologies and those without as well as skills required to use them in an efficient and safe way
- **The intertwined connection between technology and people:** deepening entangles between humans and machines in public spaces (digital roads, automated services and interfaces)

- **Intensified urbanisation** - how to keep rural communities “in the loop”
- **Expanded and exacerbated ecological destruction** - responses to which will determine how future technologies are regulated

Whether these changes will result in better or worse futures will be determined in large part by what is prioritised in technological innovation, and to what extent (if at all), previously marginalised, silenced, and exploited voices become part of the conversation. A major concern is that innovation for profit is incentivised over societal benefits. Instead, the creation and administration of smart technologies should be diversified by the communities of people who end up using the technologies. Innovation for societal benefit needs to be normalised and incentivised.

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?

Smart technologies empower people, improve their health, enhance well-being, provide accessibility services, offer proactive and pre-emptive support, and promote social connectivity and engagement. They have been successfully used to assist people, e.g., in gaining knowledge and skills, and in performing daily tasks (Sarda et al. 2022). Particularly with an ageing society they provide a viable means for enabling diverse and elderly people.

However, while such technology stands to greatly improve society, it paradoxically can also lead to increased risks, especially for the most vulnerable and marginalised in society (children, the elderly and the disabled, for example). For example, Second Sight is a company which provided bionic eyes for blind people or with visual impartment. Since that the firm discontinued its eye implants, leaving vulnerable customers in the dark and without support (Wakefield, 2022). Also, for neurodiverse people, e.g., children in the autistic spectrum, the connected and autonomous assistive robotic technology is likely to improve their skills (Sarda et al., 2022); however, we have found that much of the autonomous technologies around them are built for common use cases, disregarding neurodiversity and its effect on interaction, e.g., for natural language processing and voice-based interactions.

Smart technologies are often commercialised and made available to consumers by tech companies who do not factor in the scope of societal risks. Even smartphone apps can be created and marketed to a wide group of consumers without oversight. But research has demonstrated the need to overcome scepticism by members of the public of smart technology use and to ensure that its introduction accounts for people’s different abilities and appetite for adoption (Shirani et al, 2020). Our systematic review and experimentation relating to Autonomous Vehicles (in review - Clark et al. 2022; in the draft - Naisah et al. 2022) demonstrated greater inclination among disabled consumers toward such technology as an empowering tool. However, at the same time, we observed little research within academia and industry with a particular focus on such vulnerable groups.

Addressing inequities in the distribution of digital connectivity and equipment (the so-called ‘digital divide) (Goodman, 2020) and access to smart products and services should be fair and inclusive, and implemented in such a way that ensures that the vulnerable, and plausibly

those most in need of such technologies, are not left behind. For their fair and successful use, their design, validation, and verification should take an inclusive approach and involve diverse people throughout their development lifecycle.

It is also extremely important that the government takes the responsibility of equipping the current society with the digital skills needed to use smart technologies in a safe and efficient way (eg to manage their privacy settings or set up secure passwords) (Lisinska, et al., forthcoming). Essential Digital Skills Report 2021 showed that c.10 million (19%) of UK adults do not have fundamental digital skills (for example, be able to use a device, connect to a Wi-Fi network and create and update passwords), and c. 2.8 million people (6%) cannot do any of the foundational digital tasks. An estimated 10 million people **in the UK are excluded digitally** and are at risk of online harm when they decide to use online tools (Lloyds Bank, 2021).

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

More user research and user studies for safe, secure and user-friendly design

The government has already suggested new legislation on security for consumer IoT (DCMS et al. 2020), after it was found out that manufacturers did not build important security requirements and followed the voluntary Code of Practice for Consumer IoT Security.

In order to ensure that smart technology design is safe, secure and user-friendly, we advocate for user-centred (inclusive) research within organisations. A user-centric research places users at the centre of a device design by focusing on their needs and requirements, and the contexts in which devices are to be used. This is crucial in ensuring that technology is used by people in the most safe and secure way. For example, Alexa is a conversational voice assistant speech recognition system that collects data based on recording a user's voice input. Since being released to consumers, there have already been examples where Alexa's recordings were taken, stored, and then sent to the wrong people (Griffin, 2018). In another case, in the USA, private voice data was requested to be used for another purpose (Cuthbertson, 2018).

Technically, Amazon's Alexa is UK GDPR compliant, and users can mute their conversations, or go to their Amazon account and delete their data. Nonetheless, not everyone is aware of these functions, and the privacy capabilities are not very intuitive to use. Additionally, based on behavioural research, many people state they care about their privacy, but take very few steps to protect it in reality (Elsen et al. 2014 cited in Muravyeva et al. 2020).

Increased user research will help to encourage design that is not only secure and user-friendly but also encourages people to use devices in a way that makes sense to them, protecting their privacy and knowing the consequences of certain decisions (e.g. using weak passwords or giving consent for companies to use their data). User-centred inclusive research also incentives businesses to think about how smart technologies will be used in

practice and anticipate how design features will impact user experience, device security and safety (Lisinska et al., forthcoming).

Whilst human-centric design approaches have demonstrated significant success in creating products and services that are easy to use and accessible, recent research investment is demonstrating how next generation *More-Than-Human* Centred Design (Coulton and Lindley, 2019) approaches provide practical guidance for responding to the increasing complexity of the 21st century challenges, for example:

- Enabling data-driven product design for more equitable, sustainable products that are built around non-exploitative relationships between provider and user (Gorkovenko et al., 2020);
- Reconfiguring how technologies can be designed around sustainability and ecological concerns (Maheshwari et. al., 2022);
- Developing new models for cradle-to-cradle design (which is a design concept based on cyclical, ongoing and sustainable use of resources) to create products whose constituent parts can be repurposed and recycled at the end of their life (Stead et. al., 2020).

The UK has a uniquely strong Design Research capacity with the capability to deliver interdisciplinary, and future-focused socio-technological research at scale (Rodgers, 2020). This serves a demand in socio-technological academic research contexts, and increasingly in the private and public sectors around, for example, service and policy design. Further leveraging this capability through university collaborations with government departments has the potential to underpin proactive policy initiatives, supporting digital products and services that are environmentally, socially, and economically viable (Lindley and Coulton, 2020).

Environmental impact of smart technologies

The government has remained committed to achieving a net-zero goal. Smart technologies have an enormous potential for reducing energy costs, and some are already in use (e.g. smart meters and thermostats). Sensors embedded in smart technologies can allow the collection of energy production/consumption/storage data at high frequency and the use of this data for the optimisation of the energy systems and associated applications (Ramchurn et al, 2012). This will allow for more accurate/precise reporting of emissions by the various users and producers of energy in line with the EU Taxonomy and low carbon hydrogen standard for example.

Nonetheless, not all smart technologies are designed to bring the energy cost down (e.g. smart watches, fridges), and their positive environmental impact is not fully known due to several reasons (Lisinska et al., forthcoming):

- **Production and transportation of smart technologies:** customers do not have comprehensive information to fully be aware of how energy efficient a device is. As companies might use many components from different manufacturers and might not possess this information either (Finely, 2014). There are not enough certifications and standards.
- **Recycling and longevity**: companies are consistently creating and producing new versions of their products, but this means that many older versions may end up in landfills. This can have a negative impact on the environment by creating more waste

and releasing hazardous emissions into the environment (Finely, 2014; Gurova, 2020). New business models are needed to ensure that smart technologies do not impact the environment negatively. For example, through programs that recycle (or upcycle) older, unwanted smart technologies or redistribute these to underprivileged people in society, taking into account the need to erase all existing data from the previous user(s) and addressing the related challenges of data "leakage" into the public sphere which is also a serious problem (Schafer, 2014). Further, changes may be required to legislation to ensure that, in such business models, not only that ownership of the physical property is conveyed, but that the right to use software within the smart technology is also passed to a new owner. This is not necessarily the case currently (see Thomas, 2012)

- **Datatficiation:** (the production, processing and storage of users' data and automated data). Data centres are responsible for 2%-5% of greenhouse gas emissions globally (Mordor intelligence, 2022). Although many tech giants switch to renewable energy to reduce their carbon footprint, if data is stored locally (rather than in the cloud), this strategy will not have a huge impact on energy consumption (e.g. Lewis, 2016).

The government, in order to achieve its climate goals, needs to give careful consideration and perhaps develop policies to ensure the sustainability of smart technologies during their whole life cycle (Lisinska et al., forthcoming).

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?

Smart technologies applied well and using data and algorithms lawfully and ethically, have the potential for doing vast good and promoting human well-being. However, the impact of their application can pose serious short- and long-term challenges to human values, interests, and rights. For instance, in the case of Autonomous Vehicles, our research (Naisah et al., in draft) suggests that citizens have a greater tendency to shift blame to others or on the vehicle when accidents occur. Moreover, the regulatory ownership in such situations becomes extremely difficult to establish and thus poses significant risks for all stakeholders.

A key requirement in their deployment must be to protect the public (and the most vulnerable) and to prevent adverse outcomes - and this requirement is not always met or enforced. Significant social, legal, and ethical concerns related to smart technologies, include issues of individual freedom and personal autonomy, informed consent and transparency, and privacy, confidentiality, and data protection. It is imperative that smart systems are trustworthy – that they are legally, ethically, and technically robust – and that data are used lawfully.

We identify seven key social, legal, and ethical risks and threats.

1. **Respecting an individual's autonomy.**

Ensuring that individual autonomy is respected is critical. Individual users should maintain the ability to remain in control and manage the use of a system, influence and direct decision-making, and understand the role that such technologies play in their lives. This also speaks to the need to address the risk of over-reliance on the technology and the potential for its misuse or inappropriate use. Research at the Pew Research Centre has demonstrated how people are fearful that deepening dependence on technological systems and networks will challenge what 'it means to be human, to be productive, and to exercise free will' (Anderson & Rainie, 2018).

2. **Privacy and data protection.**

The collection of large quantities of personal data – generated by the surveillance of persons and things – comes at a cost to informational privacy. Given the potentially intrusive and vast collection, processing, storage and sharing of personal information (often, sensitive personal data or special category data) issues of digital rights, data sovereignty, and privacy and data protection arise.

As the technology is largely data-driven and data-dependent, adherence to good data protection practices and the practice of good and lawful data stewardship is paramount. This includes the collection, processing, and sharing of personal data - much of which is protected by the UK GDPR. It is imperative that users not only have full details of the nature and type of data generated but of any additional knowledge that is inferred from the data and of how such inferences are subsequently used (Watcher & Mittelstadt, 2018).

While the UK GDPR applies to the processing of personal data, certain gaps remain. An example comes from when data provided by a person has consequences that affect others. This happens when a person voluntarily discloses personal information about themselves, which exposes the personal information of others who have had no say in the matter (Koerth, 2018). This was illustrated in the Cambridge Analytica incident where participants agreeing to the access of their data in an online quiz, inadvertently allowed access to their friends' data (Guardian, 2017). Similarly, instances of health data disclosure might have significant familial implications on others, so, a mother providing information about herself, her health, or her location, might expose personal data concerning her children.

Moreover, the use of cameras and monitors for tracking and surveillance purposes and used in many smart technology applications (e.g., surveillance in smart cities), would pose a significant and increased risk of intrusion upon, and violation of, persons' privacy rights particularly if used in private spaces. What is required is a single set of clear standards by which those who develop and deploy biometric and surveillance voice and camera systems (e.g., companies, local governments, etc) will be held to account transparently and in a way that is auditable. Further clarity is required to better understand who is being held accountable and for what aspect of the smart technology lifecycle (including manufacturing, deployment, usage, data storage, data creation, data destruction, user responsibilities, companies, etc). For example, data that is generated as a purely personal or household activity, with no connections to a professional or commercial activity, would fall outside of the scope of protection afforded by the UK GDPR (DPA, 2018, Section 21(3)). This exception must be construed narrowly. As manufacturers and developers of smart devices are, almost

by definition, engaged in the development for commercial and/or professional purposes, they cannot avoid the application of the UK GDPR by invoking the household exemption (Chen et al, 2020). Where a manufacturer or developer determines the purpose and/or means of processing, and is, therefore, a data controller, either solely or jointly, they will not be permitted to rely on the household exemption.

3. Behavioural manipulation.
Smart technologies can threaten interests by using discriminatory and manipulative practices. An example of behavioural manipulation using smart technologies is that of 'nudging'. Nudging is a form of behavioural modification that is used to target and influence behaviour in a precise and effective way (Thaler & Sunstein, 2008). While nudging may be used for good and to make better choices – suppose, for example, we are nudged to eat better or to exercise more – used unethically or without consent to data collection, nudging can violate individual freedom and privacy. Nudging is often not transparent, conducted without the knowledge or consent of the user, and is both a manipulative and covertly coercive interference in decision-making (Sætra, 2019). An example of everyday nudging comes from online advertisements based on internet browsing behaviour. This is particularly problematic if the advertisement algorithms take into account online behaviour that indicates vulnerability such as searching for terms that suggest a user is disabled, suffers from mental health issues, or is dealing with addiction. The added danger is that those being manipulated are often unaware that they are being nudged. We need to ask: who is doing the nudging, for what purpose, and what are the consequences?

Moreover, people, and in particular the youth, are at risk of being used as pawns at the mercy of technology and profit-driven technology companies. Behaviour manipulation can undermine user independence and choice and compromise, rather than promote human autonomy, self-determination, and dignity. Nudging should be evaluated on the grounds of its underlying purpose and the degree to which freedom of choice is preserved.

A further example of unethical, manipulative, or unreasonably persuasive practices is the use of 'dark patterns' in website and application design (Gray et al, 2018). Dark patterns (sometimes referred to as 'anti-patterns' or 'deceptive designs') are carefully crafted user interfaces designed to coerce, steer, and deceive users into taking actions that if fully informed and offered a choice they might otherwise not have, such as purchasing overpriced products (like insurance) or signing up for recurring bills (Mathur et al., 2019). Dark patterns seek to hide, confuse, or obfuscate user choice and include, amongst other things, 'privacy zuckering' (where the user is hoaxed into publicly sharing more information than they intend to), 'confirmshaming' (where the user is guilted into opting into something), and 'bait and switching' (where the user sets about to do one thing, only to have a different and undesirable thing happen instead) (Brignull, 2017).

4. Use of voice, facial, and emotional recognition systems.
Voice, facial, and emotion recognition systems, sometimes used in smart technologies, may pose challenges to users' privacy (by intrusion into their private space), free expression (by monitoring their movements and recording their statements), and social justice (by leading to the discrimination of certain population groups). Although governed by several UK laws and regulators (such as the ICO and the UK GDPR regarding the collection and recording of facial and voice data), the circumstances and conditions under which specifically such

technologies (including the generation of synthetic content, such as deepfakes) may be used and for what purpose (if at all) both in the public and private realms should be clarified.

Speech and voice recognition technologies are used ubiquitously in many aspects of daily life. These audio-based smart technologies range from phones and in-home devices to voice-based biometric passwords for banking services and medical devices. There is growing interest in using audio technologies to automatically count occupants of buildings in order to create more efficient energy management systems. Mostly due to COVID-19, there has been a large increase in the use of video-based teleconferencing, such as Skype, Zoom, and Microsoft Teams. The same underlying methods for speech and voice technology for typical consumer products are also used in assistive technologies such as screen readers for the blind (e.g., speech synthesis), as well as audio scene analysis for the deaf (e.g., speech/audio recognition). Furthermore, synthetic speech that is generated by a computer or machine has applications in the creative industries (e.g., creating character voices) as well as to help people who have lost their ability to speak (through injury or disease) and who require voice reconstruction.

Studies show that consumers have already expressed concerns about feeling monitored or surveilled by these technologies (Easwara Moorthy and Vu, 2015; Balamurali et al., 2019). In addition, people may even modify their behaviour, or whisper, when they think that they are near a smart audio device (Vimalkumar et al., 2021). Consumer concerns are of merit. It takes only 3-5 seconds of recorded speech audio to create an audio “deepfake” that is powerful enough to “trick” voice authentication systems like those used to verify identity in banking (Luong and Yamagishi, 2020). An audio deepfake is speech that was generated by a computer algorithm, or snippets of real speech taken out of context and re-arranged for malicious purposes. Technology companies have been allowed to widely commercialise speech and audio products without oversight, and without regard to additional consumer protections. In academic research, the dangers of speech technology are well-known among academics who are conducting fundamental research. These concerns are so strong that in 2015 the speech research community self-organised an international biennial meeting to present work that counters voice-based cyberattacks, including audio deepfake detection (Wu et al., 2015). In fact, it was decided in 2020 that additional meetings were needed among academics to address a specific and dangerous aspect of voice privacy information found in speech (Tomashenko et al., 2020). Despite progress from academics, none of these protective countermeasures are deployed in commercial speech products that consumers can purchase (e.g., Alexa, Google Home, smart phones, smart watches, etc), and technology companies are not incentivised to provide additional protections.

5. Preventing cyberattacks and data breaches.

Greater use of smart technologies demand hacking and cyber security protections. Poorly secured smart products and services threaten persons’ online security, and subsequently, their privacy and safety. Cyberattacks can result in economic loss and have wider implications for society and the national economy.

Related to our second point on privacy and data protection, cyberattacks and data breaches can expose data that individuals may otherwise consider private or confidential when using a smart service. For example, there are many different kinds of apps that can be downloaded (often for free) that help a woman track her ovulation cycle (e.g., Natural Cycles, Mira, Flo,

Glow, Fertility Friend, etc). Not only is this data-sensitive, but some women would also consider it to be private information that they are using such an app at all. This and similar smart technologies capture information that consumers may mistakenly believe is protected from cyberattacks without a full understanding of the implications if they participate in a smart service.

It is becoming increasingly difficult to opt-out of certain smart services. For example, many banks in the UK and Europe are starting to use voice-based biometrics in order to access services via telephone. These services require a patron to speak a passphrase such as, “My voice is my password.” While this form of biometric identification is advertised as being safe and secure by the banking institutions, the banks do not fully inform their customers of the risks of biometric voice spoofing (also called voice “deepfakes”, which means manipulating the speech of an original user to breach the security of a device or the security of accessing services) that are well-known in the academic community. In the same way that large tech companies are not held to account for privacy related to in-home voice assistants, banking institutions that use speaker voice biometrics are not legally required to provide protection against voice deepfakes, which can be used as a form of a cyberattack against individuals.

6. Developing common mental models
Smart technologies are complex by nature. The introduction and continuous evolution of these devices make it difficult for citizens to keep abreast with changes that occur within a short span of time. For instance, the smartphone which evolved from a fairly basic device a decade and a half ago has spawned into unique platforms and ecosystems. Many of these ecosystems have created barriers in terms of functionality and interchangeability. For instance, an Apple user will not be able to use many software such as purchased apps and peripheral devices such as chargers for Android-based smartphones. Thus, without common mental models or frameworks, stakeholders cannot find a common ground to operationalise and understand the nature of such technology. It may lead to substantial levels of consumer confusion (Wang & Shukla, 2013) which in turn may create technological silos, incomparability of practice and numerous risks for all stakeholders involved.

7. Mixed-Initiative decision-making and Provenance Tracking
Autonomous systems will increasingly work alongside humans or take over human decision-making in a range of settings (e.g. autonomous vehicles, recruitment systems, emergency response planning and response). In many cases decisions will be made at machine speed, making it difficult for humans to understand the complex set of inputs machines take into account in making decisions alongside humans. In other cases, chains of decisions involving humans and machines will add more opacity to human-machine systems that impact on our daily lives. Unless data and decisions are tracked in such systems (i.e, the provenance of decisions) it will leave humans and organisations exposed to ethical risks with they may not be responsible for nor equipped to deal with (Ramchurn et al., 2021).

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?

In combination, regulatory, policy-development, guidance measures, and increased awareness and education can be used to overcome the concerns raised above. These concerns can be managed and mitigated through an effective governance regime.

Although there are existing frameworks and promulgated and draft legislation applicable to smart technologies such as, amongst others, the:

- UK General Data Protection Regulation and the Data Protection Act 2018, which protect personal data and provide a mechanism for addressing data breaches,
- Consumer Protection from Unfair Trading Regulations 2008 and Consumer Rights Act 2015, which provide a framework of rights and obligations relating to consumer products, creates a framework for civil and criminal liability and sets out powers relating to a criminal investigation of breaches of consumer law,
- General Product Safety Regulations 2005, which provide that all products placed on the market should be reasonably safe, and
- Product Security and Telecommunications Infrastructure Bill, which seeks to secure against cyberattacks and allows for the provision of mandatory security requirements,

they do not go far enough in addressing the unique risks posed by smart technologies.

For instance, data protection legislation does not protect against the harms of inferential analytics or provide a clear right to an explanation (Watcher, 2019; Watcher et al, 2017). Policy guidance and development are required to:

- clarify the circumstances and conditions under which voice, facial, and emotional recognition systems might be used (if at all);
- clarify whether and for what purpose systems may be used to generate synthetic content or manipulate image, audio, or video content, including deepfakes;
- address how to enforce protection from deepfakes through a combination of technical solutions (e.g., to detect deepfakes in the first place) and legal and/or ethical solutions;
- consider and address whether widely commercialised speech and audio products (such as Alexa) require additional consumer protections and ethical or other oversight;
- implement educational initiatives to ensure consumers understand what they are consenting to, and why data requires protection;
- ensure greater transparency and clear disclosure requirements, including informing users in less obvious cases that they are interacting with a bot (so-called ‘bot disclosure’);
- provide clear guidance on commitments to explainability, accountability, and responsibility attribution models;
- provide a framework for validating and verifying ethical concerns such as fairness and bias;
- address power asymmetries which arise between users and various data players (typically technology organisations and third-party platforms) and limit and control vast repositories of privately collected data by unaccountable parties (Zuboff, 2019; Véliz, 2020); and
- curtail objectionable behavioural manipulation practices (such as inappropriate nudging) by unethical actors.

Consumer law could consider how to address goods containing embedded software, and consider whether the provisions relating to digital content in the Consumer Rights Act are (already) outdated. There could also be consideration of whether the need, in the Consumer Protection from Unfair Trading Regulations 2008, to prove that a misleading or aggressive practice would have resulted in an average consumer taking a transactional decision they would not otherwise have made provides a barrier to regulating undesirable practices involving smart technologies.

Smart technologies raise important **social and ethical concerns** which have application, more generally, to AI-based and other technological system design, development, and deployment. There are gaps in the regulatory framework and the policy landscape is fragmented. In light of this, current regulatory frameworks may need to be reviewed to ensure that there is clear responsibility for overseeing all aspects of smart technologies and that those charged to do so can do so effectively across all domains. Importantly and relatedly, the standards and guidelines do not account for the very many ethical concerns arising from smart technology applications.

The question of whether these normative issues should be managed by policy prescriptions, verification, validation and audit requirements, or for political reasons are best left to self-regulation and aspirational ethics rather than enforced through law is unclear. Comprehensive and specific policies that go beyond general national laws and that set clear standards may be needed – such as the development of Codes for smart devices or smart cities, for example, and the need for specific legal and ethical guidance (on disclosure and transparency requirements, issues of fairness and social and distributive justice, system trustworthiness, responsibility and accountability, and guidance on the assessment and reporting of automated decision systems). Ethics-based and algorithmic impact assessments, assurance models, audit tools, and oversight measures can also be implemented so that those technologies at high-risk for human rights infringements can be detected and managed or prohibited. The indicated normative issues point to threats and concerns with automated decision-making systems and AI-based technological adoption, more broadly, requiring, we suggest, urgent consideration.

References

Anderson, J. & Rainie, L. (2018). Artificial Intelligence and the Future of Humans. Artificial Intelligence and the Future of Humans | Pew Research Center. (Accessed 15 June 2022).

Balamurali, B.T., Lin, K.E., Lui, S., Chen, J.M. and Herremans, D. (2019). Toward robust audio spoofing detection: A detailed comparison of traditional and learned features. *IEEE Access*, *7*, pp.84229-84241.

Bogost, I. (2022) 'Google's Sentient Chatbot is Our Self-Deceiving Future', The Atlantic, available at https://www.theatlantic.com/technology/archive/2022/06/google-engineer-sentient-ai-chatbot/661273/

Brignull, H. (2017) "Types of Dark Patterns". Available from: https://www.deceptive.design/ (Accessed 20 June 2022).

Clark, J., Naiseh, M., Akarsu, T., Hanoch, Y., Wald, M., Brito, M., Webster, T. & Shukla, P. (2022). Trust, Risk Perception, and Intention to Use Autonomous Vehicles: A Bibliometric Review, *Under review*.

Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020) Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law*, *10*(4), 279-293.

Coulton, P. and Lindley, J. G. (2019) 'More-Than Human Centred Design: Considering Other Things', The Design Journal, pp. 1–19. doi: 10.1080/14606925.2019.1614320.

Cuthbertson, A. (2018) Amazon ordered to give Alexa evidence in double murder case. The Independent,14th Nov. Available from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-echo-alexa-evidence-murder-case-a8633551.html. Accessed 01/11/2021

DCMS et al. (2020) *Government to strengthen security of internet-connected products.* Available from: https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products. Accessed 02/08/2021.

Easwara Moorthy, A. and Vu, K.P.L.. (2015) Privacy concerns for use of voice activated personal assistant in the public space. *International Journal of Human-Computer Interaction*, *31*(4), pp.307-335.

Finely, K. (2014) The Internet of Things Could Drown Our Environment in Gadgets. Wired. 06th May. Available from: https://www.wired.com/2014/06/green-iot/.

Gaur, B., Shukla, V. K., & Verma, A. (2019). Strengthening People Analytics through Wearable IOT Device for Real-Time Data Collection. 2019 International Conference on Automation, Computational and Technology Management, ICACTM 2019, 555–560. https://doi.org/10.1109/ICACTM.2019.8776776

Goodman, EP. (2020) Smart City Ethics in *The Oxford Handbook of Ethics in AI*. 836.

Gorkovenko, K. et al. (2020) 'Exploring The Future of Data-Driven Product Design', in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM, pp. 1–14. doi: 10.1145/3313831.3376560.

Gray, Colin M.; Kou, Yubo; Battles, Bryan; Hoggatt, Joseph; Toombs, Austin L. (2018). "The Dark (Patterns) Side of UX Design". *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. New York, New York, USA: ACM Press: 1–14.

Griffin, A. (2018) How an Amazon Echo recorded a family's private conversation then sent it to a random person. *The Independent,* 25th May. Available from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-echo-recording-alexa-message-family-security-stop-how-to-a8369311.html. Accessed 01/11/2021

Guardian. 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach'. 17 March 2017. Available from: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (Accessed 13 June 2022).

Gurova, O., Merritt, T. R., Papachristos, E., & Vaajakari, J. (2020) Sustainable solutions for wearable technologies: Mapping the product development life cycle. *Sustainability* (Switzerland), 12(20), 1–26. https://doi.org/10.3390/su12208444

Koerth, K. (2018) 'You Can't Opt Out Of Sharing Your Data, Even If You Didn't Opt In' *FiveThirtyEight.* 3 May 2018. Available from: https://fivethirtyeight.com/features/you-cant-opt-out-of-sharing-your-data-even-if-you-didnt-opt-in/ (Accessed 12 June 2022).

Lewis, D. (2016) *Will the internet of things sacrifice or save the environment?* Available from: https://www.theguardian.com/sustainable-business/2016/dec/12/will-the-internet-of-things-sacrifice-or-save-the-environment (Accessed 15 June 2022).

Lindley, J. and Coulton, P. (2020) AHRC Challenges of the Future: AI & Data.

Lisinska (Jonak), J., Weerawardhana, S. Kleinman, M. (Eds) (2022) *Trusted Internet of Things at home and in the workplace: A policy landscape review*. DOI: 10.18742/pub01-084 *Forthcoming.*

Lloyds Bank (2021) *Essential Digital Skills Report 2021*. Available from: https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/211109-lloyds-essential-digital-skills-report-2021.pdf. Accessed 11/12/2021.

Luong, H.T. and Yamagishi, J., (2020) Nautilus: a versatile voice cloning system. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *28*, pp.2967-2981.

Maheshwari, A., Kumar Aggarwal, A. and Danielescu, A. (2022) 'Designing Tools and Interfaces for Ecological Restoration: An Investigation into the Opportunities and Constraints for Technological Interventions', in *CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 1–17. doi: 10.1145/3491102.3517664.

Mathur A, Acar G, Friedman M, Lucherini E, Mayer J, Chetty M, Narayanan (2019) A: Dark patterns at scale: findings from a crawl of 11K shopping websites. *ACM Conf. Comp.-Supported Cooperative Work 2019.*

Mordor Intelligence (2022) *Data Centre Cooling Market - Growth, Trends, COVID-19 Impact, And Forecasts.* Available from: https://www.mordorintelligence.com/industry-reports/global-data-center-cooling-market-industry.

Muravyeva, E., Janssen, J., Specht, M. et al. (2020) Exploring solutions to the privacy paradox in the context of e-assessment: informed consent revisited. *Ethics Inf Technol* 22, 223–238. https://doi.org/10.1007/s10676-020-09531-5

Naiseh, M., Clark, J., Akarsu, T., Hanoch, Y., Wald, M., Brito, M., Webster, T. & Shukla, P. (2022), Intention to use Autonomous Vehicles (AVs) under uncertain situations, *draft*.

Ofer, N., Bell, F. and Alistar, M. (2021) Designing Direct Interactions with Bioluminescent Algae', in *Designing Interactive Systems Conference 2021*. New York, NY, USA: ACM, pp. 1230–1241. DOI: 10.1145/3461778.3462090.

Ramchurn S. D, Vytelingum P., Rogers A. , and Jennings N. R (2012) Putting the 'smarts' into the smart grid: a grand challenge for artificial intelligence. Commun. ACM 55, 4 (April 2012), 86–97. https://doi.org/10.1145/2133806.2133825
Ramchurn SD, Stein S, Jennings NR. Trustworthy human-AI partnerships. iScience. 2021 Jul 24;24(8):102891. doi: 10.1016/j.isci.2021.102891. PMID: 34430804; PMCID: PMC8365362.
Rodgers, P. (2020) AHRC Design Leadership Fellowship Final Report.
Sætra, HS (2019). 'When nudge come to shove: Liberty and nudging in the era of big data' *Technology in Society.* 59(101130)1.
M. Sarda Gou, G. Lakatos, P. Holthaus, L. Jai Wood, M.R. Mousavi, B. Robins, and F. Amirabdollahian. Towards understanding causality – a retrospective study of using explanations in interactions between a humanoid robot and autistic children. Proceedings of the 31st IEEE International Conference on Robot & Human Interactive Communication (RO-MAN 2022), IEEE, 2022.
Schafer, B. (2014). D-waste: data disposal as challenge for waste management in the Internet of Things. *The International Review of Information Ethics*, *22*, 101-107.
Shirani, F. Groves, Cr. Henwood, K., Pidgeon, N., Roberts, E. (2020) 'I'm the smart meter': Perceptions of smart technology amongst vulnerable consumers. *Energy Policy*. 144, 11163.
Stead, M., Gradinar, A. and Coulton, P. (2020) 'Must All Things Pass? Designing for the Afterlife of (Internet of) Things', ThingsCon The State of Responsible Internet of Things Report.
Thaler RH & Sunstein CR (2008) *Nudge*. London: Penguin Books.
Thomas, S. (2012) Goods with embedded software: obligations under Section 12 of the Sale of Goods Act 1979. *International Review of Law, Computers & Technology*. 26:165-183
Tomashenko, N., Srivastava, B.M.L., Wang, X., Vincent, E., Nautsch, A., Yamagishi, J., Evans, N., Patino, J., Bonastre, J.F., Noé, P.G. and Todisco, M.. (2020) "Introducing the VoicePrivacy Initiative". In *INTERSPEECH 2020*.

Véliz, C. (2020) *Privacy is Power.* London, UK: Penguin (Bantam Press).

Vimalkumar, M., Sharma, S.K., Singh, J.B. and Dwivedi, Y.K. (2021) 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, p.106763.

Wachter, S., Mittelstadt, B., Floridi, L. (2017) Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law* 1.

Wakefield, J. (2022) *Bionic eyes: Obsolete tech leaves patients in the dark*. Available from: https://www.bbc.co.uk/news/technology-60416058

Wang, Q., & Shukla, P. (2013) Linking sources of consumer confusion to decision satisfaction: The role of choice goals. *Psychology & Marketing*, *30*(4), 295-304.

Watcher, S. (2019) Data Protection in the Age of Big Data. *Nature Electronics*. 2:6-7.

Watcher, S. & Mittelstadt, B. (2018) A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review.*

Wu, Z., Kinnunen, T., Evans, N., Yamagishi, J., Hanilçi, C., Sahidullah, M., & Sizov, A. (2015) ASVspoof 2015: the first automatic speaker verification spoofing and countermeasures challenge. In *INTERSPEECH* 2015.

Zuboff, S. (2019) *The Age of Surveillance Capitalism*. Profile Books.