UKRI Trustworthy Autonomous Systems Hub
The University of Nottingham
University of Southampton
The Policy Institute
King's College London

Trusted Internet of Things at home and in the workplace

A policy landscape review

Justyna Lisinska and
Sachini Weerawardhana

July 2022

About the UKRI TAS Hub and TAS Programme

The UKRI TAS Hub assembles a team from the Universities of Southampton, Nottingham and King's College London. The UKRI TAS Programme is a four-year multi-disciplinary research programme worth £33m, funded by UKRI through the Strategic Priorities Fund. It is the world's largest research programme in Trustworthy artificial intelligence (AI) and autonomous systems.

The vision of the programme is to enable the development of socially beneficial autonomous systems that are trustworthy in principle and trusted in practice by the public, government, and industry. The TAS Programme currently involves more than 20 Universities, and more than 130 researchers from over 10 disciplines engaging with over 180 industry partners. Read more about the TAS Hub here.

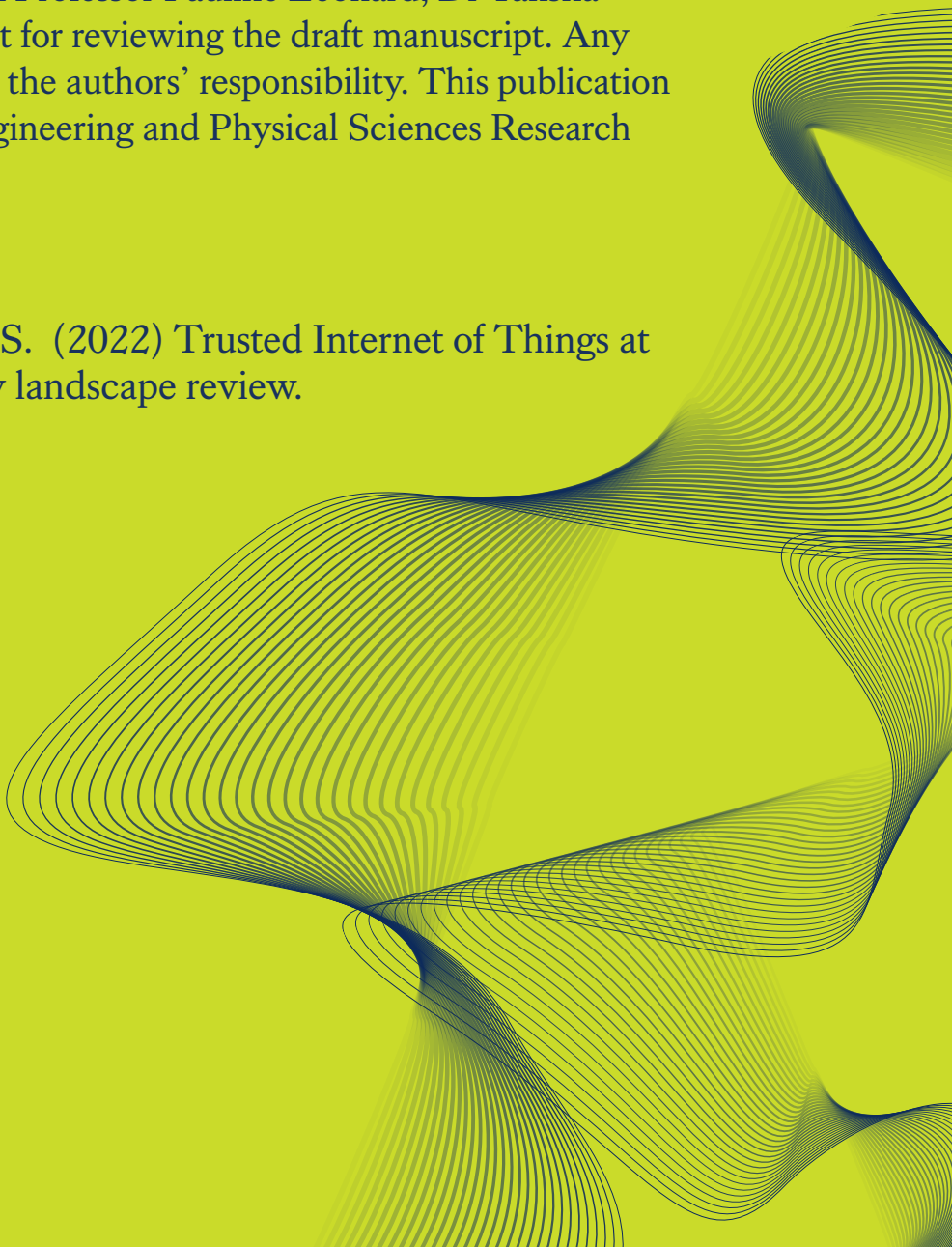
Acknowledgements

The authors would like to thank Professor Pauline Leonard, Dr Yansha Deng, and Dr Lachlan Urquhart for reviewing the draft manuscript. Any errors or omissions are of course the authors' responsibility. This publication acknowledges funding from Engineering and Physical Sciences Research Council (EP/V00784X/1).

Citation

Lisinska, J., Weerawardhana, S. (2022) Trusted Internet of Things at home and workplace: a policy landscape review.

DOI:10.18742/pub01-084



Abbreviations

AI	Artificial intelligence
AI Act	The European Commission's Artificial Intelligence Act
AS	Autonomous systems
BEIS	Department for Business, Energy and Industrial Strategy
DCMS	Department for Digital, Culture, Media and Sport
EC	Edge computing
ETSI	European Telecommunication Standards Institute
GDPR	The General Data Protection Regulation
H2H	Human to human
H2T	Human to thing
ICO	The Information Commissioner's Office
IoT	Internet of Things
IRTF	The Internet Research Task Force
T2T(s)	Thing to thing(s)
TAS Hub	Trustworthy Autonomous Systems Hub

Executive summary

This report is a horizon scanning of issues arising from the application of autonomous systems (AS) in the domain of the Internet of Things (IoT) at home and in the workplace, produced for Trustworthy Autonomous Systems Hub (TAS Hub). The role of the TAS Hub is to help the UK deliver world-leading best practices for the design, regulation and operation of AS, which are trustworthy and socially beneficial.

As we enter the fourth industrial revolution, IoT – and how people adopt it – transforms how we live, communicate and conduct businesses. Such a transformation is likely to bring issues where government, industry and researchers need to respond. In our policy landscape review, we explore the main policy issues the government should focus on and provide areas for further research.

Our key findings fall into seven main areas:

1. Definition of IoT and AS

There is no set definition of IoT, where the community – consisting of researchers, academics, and industry – focuses on the different capabilities of IoT. We review the definition of IoT from a technical and government perspective to be able to understand what AS mean in the context of IoT.

From the technical approach, we learn that autonomous systems are "things" connected to the internet that have sensing/actuation capabilities to monitor the physical space and take action. For example, robot vacuum cleaners are connected to the internet, can be managed from a mobile phone or smart speaker and are able to scan the environment to detect things and obstacles.

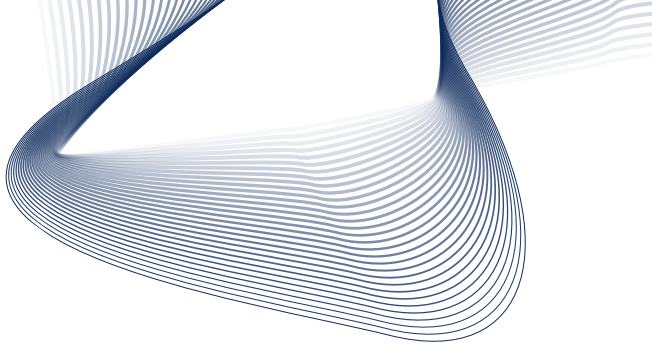
From a policy perspective, IoT is about human and non-human interactions. IoT is meant to help humans to make more intelligent decisions. We view both definitions as correct; we consider IoT as a social-technical phenomenon where both social and technical factors are at play. Therefore, to address the problems discussed below, academia and the government need to collaborate with different stakeholders to design the best solutions.

2. Trust in IoT

From a technical standpoint, a key challenge is the absence of a unified, well-developed, and widely adopted model of trust. The trustworthiness of an IoT environment depends not only on the data and the communication among heterogeneous devices in the network, but also on human user interactions.

We recommend that IoT trust models should be developed to standardise the different interaction models in the IoT environment: between the human and the devices and between the devices themselves. Special focus must be given to the diverse human user groups in the IoT environments: device manufacturers, IoT service providers, application developers, retailers, and end-users.

We suggest a discussion to define a spectrum of autonomy in IoT devices as a precursor to standardising trust in IoT. For example, the SAE Levels of Driving



Automation defines the levels of human engagement in an autonomous vehicle, which can be used to frame the discussion on trust in the automation.

We also suggest that trust in IoT should take into consideration psychological aspects and public attitudes, especially when considering a wide adoption of IoT's products and IoT automation solutions. Technological development is not set in stone or pre-determined. Historically, examples have shown that lack of public acceptance can negatively impact the pace and direction of scientific activity and innovation.

3. Lack of clear strategy for IoT

Although there are strategies issued by the government that relate to IoT (eg *National AI Strategy* or *the UK Innovation Strategy*), there is a lack of a specific strategy and regulation for this sector in the UK.

The exception is the development of new legislation to protect smart devices in people's homes from being hacked. This new law was initiated after it was found out that many manufacturers have ignored the voluntary Code of Practice for Consumer IoT Security. There are also more general regulatory frameworks. For example, ETSI EN 303 645 V2.1.1 is an influential standard framework that was developed with industry, academics, testing institutes and international government bodies for consumer IoT security standards.

4. Environmental impact

IoT can offer a vast potential to reduce energy consumption in the home or office. Nonetheless, not all smart devices that can be used in the home and office are designed to bring energy costs down. What is more, the environmental impact of IoT – through manufacturing, transportation and production – is not fully known.

We advise that the government works with different stakeholders to understand the impact of smart devices on the environment to ensure that a Net Zero goal can be achieved.

5. Security and product liability

Smart devices raise security issues that impact online and offline realms, as well as humans. Comprehensive security solutions are very often comprised at the expense of low memory space and energy. The government proposed legislation on security requirements of IoT after many manufacturers failed to build necessary security requirements, however, product liability in case of data and security breaches has not been established – this should change.

In academia, researchers have worked on different technical solutions to mitigate security risks. More recently, a user-centric IoT approach has been proposed where a user is put at the centre of the design. This approach also allows people to be in charge of their own information.

6. Data, privacy and ethical issues

At home

There have been examples of privacy concerns when a smart device, such as Amazon's Alexa, collected information later used for a different purpose, misheard the wake-up word (after which conversations can be recorded), or sent recorded data to the wrong people. Although technology can make mistakes, these examples undermine trust in IoT and public acceptance.

Amazon has introduced features where users can customise their privacy settings. But we draw attention to the fact that people might not be aware of the need to change/check their privacy options and know how to do it, even when such an option exists. We also point to a discrepancy in users' views on privacy and their actual behaviour, based on online behaviour research. People who state they are concerned about privacy take few steps to protect it.

This issue leaves policymakers with a difficult question of how users' privacy should be protected when they voluntarily disclose their information. We advise that policymakers work with diverse stakeholders since privacy is a complex, often contextual topic and encourage more user-centred studies where users' behaviour is investigated.

In the workplace

We discuss policy issues mainly from the perspective of new ways of monitoring employees' activity. With the pandemic and more people working from home, employers started utilising digital tools to monitor workers at home. Even though cameras are now mainly used to monitor workers at home, new, more sophisticated smart devices are likely to be used if flexible working continues to be popular.

The Information Commissioner's Office (ICO) provides *The Employment Practice Code* with a section on monitoring; however, the guidance does not refer to new ways of monitoring workers at home. In turn, research has mainly focused on studying productivity in terms of workplace surveillance, but less attention was given to data justice, which means fairness in the way people are made visible, represented and treated as a result of their production of digital data (see Azer, 2021).

7. Skills and jobs

Although the government considers the skills needed to develop AI systems (eg the *National AI Strategy*), these plans are not directly aimed at supporting workers whose tasks become displaced by IoT systems. What is more, people also need to be digitally literate in order to use smart things correctly and avoid risks, eg update passwords or manage privacy.

The *Essential Digital Skills Report 2021* shows that 19 per cent (c.10 million) of UK adults do not have fundamental digital skills, such as using a device, connecting to a Wi-Fi network, or creating and updating passwords. As a result, an estimated 10 million people are digitally excluded and at risk of harm when they go online.

Introduction

The introduction of the internet has changed how people do business, communicate, interact with services, and access information (Dutton, 1999). The IoT builds on such transformation, with the internet "increasingly used to link devices, machines and other objects" (Dutton, 2014: 2).

However, IoT is not a new concept; it was first coined by a British technologist pioneer Kevin Ashton as early as 1999 (Kramp, 2013). The development of IoT is linked with the fourth industrial revolution. The first revolution considered the usage of water and steam power to mechanise production; the second created mass production by using electric power; and the third revolution relied on electronic and information technology for automating production (Schwab, 2016). The fourth industrial revolution blurs the lines between the physical and digital worlds (BEIS, 2019; Schwab, 2016).

There has been a continuous growth in cellular IoT connections; their number had grown from 76 million in 2010 to 1,102 million in 2018 (Edquist et al., 2021: 264). During the pandemic, the purchase of smart devices increased in the UK. These higher demands, among other factors, contributed to the problem of the global shortage of computer chips, an essential component of smart devices (Gregersen, 2021). Therefore, the chip shortage might mean lower growth in the industry in the coming years.

While IoT has many applications in different sectors, this report focuses on the use of IoT at home and in the workplace, which brings enormous opportunities to assist us in our daily lives and increase our productivity. IoT can also contribute to reductions in carbon emissions. For example, emissions can be reduced by optimising the energy flows of buildings, appliances, and buildings' energy systems (Record Evolution, n.d.). The UK government introduced in law a target to reduce emissions by 78 per cent by 2035, as part of the Net Zero strategy by 2050 (BEIS et al., 2021).

However, a vast number of devices connected to the internet could also negatively impact the environment. Both in terms of the amount and type of energy used by data storage companies, and also because any old device replaced by an intelligent device would need to be disposed of. IoT is not everlasting, and its use is not limited to only saving energy consumption (Finely, 2014). Furthermore, smart devices raise a lot of questions around security – security risks that impact online and offline environments and humans; data and privacy; skills – skills needed for production, maintenance of IoT, and digital literacy; and jobs – jobs replaced by smart things.

Our approach

The aim of this policy landscape is to provide policymakers and researchers with key issues arising from the application of IoT systems at home and in the workplace. We present a high-level analysis from scanning the grey literature, as well as available academic literature. As such, this review is not an exhaustive, systematic review.

In the following sections, we first define IoT and autonomous systems, and then we review their potential applications at home and in the workplace. Next, we map the policy landscape in the UK concerning IoT. We finally discuss the associated policy

issues grouped under four themes: **reducing carbon emissions**; **security**; **data, privacy and ethical issues**; and **skills and jobs**.

Defining concepts

IoT and AS

There are several approaches to defining IoT. This paper presents a technical perspective and a definition used in the government's publications of how IoT should be defined. We did not select these two definitional approaches without reason. First, the government's view on how IoT is defined considers a human factor – either IoT should help people make more intelligent decisions, or its definition highlights the relationship between human and non-human objects. In turn, a technical approach describes the technical capabilities of IoT, enabling us to see what AS are in the context of IoT.

Starting from the government's perspective, Jonny Voon, Head of The Sustainable Innovation Fund at Innovate UK, wrote that, for him, IoT is:

> *"Where connected objects share their data and derivable, actionable insights to help make smarter decisions for the benefit of humans."* (Voon, 2016)

A similar approach is echoed in the definition provided in the Blackett review (a process for government to engage with academia and industry to work on a specific issue or question):

> *"The IoT describes a world in which everyday objects are connected to a network so that data can be shared. But it is really as much about people as the inanimate objects."*
> (Government Office for Science, 2014)

We can see that these two perspectives on IoT are very similar to each other and have a pre-assumption that **objects are connected and share their data**. There is also a reference to the intertwined connection between people and objects.

IoT systems will always have machine-to-machine (M2M) solutions (Edquist, et al. 2021: 264), but as Höller et al. (2014) pointed out, they do not necessarily enable data sharing or connect devices to the Internet. Additionally, Silverio-Fernández (et al. 2018: 10) argues that:

> *"The core ideas of the IoT are that devices interact with other devices, not necessarily people; hence the name 'Internet of Things,' an internet designed for things, not people."*

Nonetheless, that does not change the fact that IoT should be beneficial for society and trusted by the public. It is also worth mentioning that IoT is a socio-technical construct where social and technical factors influence each other, so technology is not produced in a vacuum. As Carlson (1994: 161) noted, "the 'end-use' of technology is created or constructed by a variety of participants in a technological enterprise". Thus, it can be said it is true IoT is *"really as much about people as the inanimate object"* (Government Office for Science, 2014).

This concept of co-constitution and mutual shaping was developed as a critique of early studies that viewed technology as a source of societal changes (MacKenzie & Wajcman, 1999; Halford et al., 2010). The approach where technology develops by following a predictable logic of science, away from social influences and technology,

and determines social changes was also referred to as technological determinism (Kline, 2001: 15495).

Looking at the technical definition of IoT, the IEEE paper Toward a Definition of Internet of Things (IoT) suggests that:

> *An IoT is a network that connects uniquely identifiable 'things' to the internet. The 'things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'thing' can be collected, and the state of the 'thing' can be changed from anywhere, anytime, by anything."* (Minerva et al. 2015)

The "things" can be defined as **objects** connected to the internet. Compared to previously mentioned definitional approaches to IoT, the above definition helps to understand what connected things/objects are designed to do. From this definition, we can learn that AS/devices have sensing/actuation capabilities to monitor the physical space and take action (US Department of Defence, 2016: 1).

The TAS Hub defines an AS in a general sense as a "system involving software applications, machines, and people, that is able to take actions with little or no human supervision" (TAS-Hub, 2020). In this paper, we define the "things" as autonomous systems that take actions with "little or no human supervision" (TAS-Hub, 2020). "Things" in IoT are also often referred to smart devices, mobile devices, smart things or smart objects in the academic literature (Silverio-Fernández et al. 2018: 10).

However, it must be pointed out that in technical terms, sensors/actuators are only one part of a wider IoT technical environment. OECD (2018:10) distinguished four key enablers for IoT to function:

- semi-conductors (eg sensors, chips, processors, memory, and so forth);
- modules and devices (eg software/API connecting the IoT devices);
- IoT platforms (eg operating systems to support IoT solutions);
- the network (eg connectivity where standardisation and interoperability issues are relevant).

Apart from the technical environment, the IoT also comprises physical (human and non-human objects and physical surroundings) and social-economic (eg consumers, legislative bodies, businesses) environments (Arthur, 2017). In the next section, we explore what we mean by trust in IoT based on the definition developed by the TAS-hub.

Trust in IoT

The TAS Hub (2020) defines autonomous systems as trustworthy when "their design, engineering, and operation ensures they generate positive outcomes and mitigates potentially harmful outcomes." Some of the factors that influence the trustworthiness of autonomous systems are:

- Their **robustness** in dynamic and uncertain environments.

- The **assurance of their design** and operation through verification and validation processes.
- The **confidence they inspire** as they evolve their functionality.
- Their **explainability, accountability, and understandability** to a diverse set of users.
- Their **defences** against attacks on the systems, users, and the environment they are deployed in.
- Their **governance** and the **regulation** of their design and operation.
- The consideration of **human values and ethics** in their development and use.

(Ibid.)

Intertrust Technologies (2010) writes that people need to trust the security, safety, and privacy of IoT. Thus, technologists must work towards intuitive and simple design to help people understand devices' and services' capabilities, as well as possible threats. Various scientists are working on different trust models, but as the authors note, there is no one unified, well-developed and widely adopted model to be used by IoT designers and engineers (ibid.). There is a question, however, of whether there can or should be one trust model that considers the different needs and requirements of people that engage with IoT devices.

As previously discussed, from a technical perspective, the "things" of the Internet of Things refer to heterogeneous computing devices connected together over the internet. The communication between these devices has been standardised by protocols, such as the European Telecommunication Standards Institute (ETSI) (see: DCMS, 2019). Standards allow the communication between the devices to happen in a meaningful way despite the heterogeneity in the network. However, not much work has looked at standardising trust in IoT environments, specifically focusing on users who have different needs and motivations interacting with the devices on the network. Trust establishment, measurement, maintenance, and repair are key challenges in IoT environments because, as with the devices, human users also leave and join the network in an ad-hoc manner.

For both home and workplace environments, we recommend that trust in IoT must be studied on different interaction models: between the person and the device, and between the devices. The Internet Research Task Force (IRTF) identifies that an IoT environment consists of a number of different communication patterns: human-to-human (H2H), human-to-thing (H2T), thing-to-thing (T2T) or thing-to-things (T2Ts) (Garcia-Morchon, et al. 2019). Entities participating in any of the interaction models may have a different understanding of trust. It is important that these differences are reconciled in a standardised way during the interaction. Trust in data is as important as the trust between humans and devices in the IoT.

The Internet Society Online Trust Alliance recognises that IoT environments have a diverse set of stakeholders: device manufacturers, IoT service providers, application developers, retailers, and end users (ISOC-OTA, 2018). Therefore, policy frameworks addressing IoT trust need be based on a broad understanding of

the stakeholders and their complementary and/or conflicting requirements of trust in IoT environments.

We encourage a discussion to define a spectrum of autonomy in IoT devices as a precursor to standardising trust in IoT. For example, the SAE Levels of Driving Automation (SEA, 2022) defines the levels of human engagement in an autonomous vehicle, which can be used to frame the discussion on trust in the automation. Is there a difference between the expectations of trust from an IoT device that gathers and reports data to an IoT gateway, compared to an IoT device directly sending data to an autonomous system – eg an autonomous car or an industrial robot? A systematic approach for classifying the IoT devices based on the data, not only considering where it originates, but also what happens to the data the device receives and disseminates, is a necessary first step in understanding how to build trust in the IoT environment.

Trust in data is as important as the trust between humans and devices in the IoT. This is because data disseminating IoT deployed "in the wild" can create unintended and perhaps dangerous situations. For example, The Wall Street Journal reported an issue with Apple's AirTag tracking, which resulted in iPhone users receiving alerts for unknown AirTags; a form of AirTag Stalking (Brown, 2022).

Although IoT brings new trust challenges, where traditional security and privacy solutions are not enough, we want to highlight that trust in any technology should go beyond technical issues that might impact the adoption of IoT products. The technological development of IoT systems is not set in stone or pre-determined (see: Winickoff, 2017).

Historically, public resentment has negatively impacted the direction and pace of scientific activity. For example, in Europe, negative public perception of genetically modified organisms (GMO) resulted in lower funding levels and high regulatory rejection rates (Currall et al., 2006). Therefore, we suggest that public concerns should be taken into account when developing trust in IoT systems and trust be considered as a multifaceted concept, rather than a technological fix.

As Winickoff (2017) observes, resistance to adoption of technological innovation might come from value conflicts, distributive concerns, and failures of trust in governing institutions. To build trust and trustworthiness into the technical system, Winickoff (2017) recommends utilising participatory forms of foresight and technology assessment, and engaging stakeholders in communication processes.

IoT applications

IoT has a wide range of applications. Hassan et al. (2020), based on a review of different studies, distinguished six main sectors: healthcare (eg smart wearables); infrastructural (eg real-time performance, or energy efficiency); environmental (eg smart farming); industrial (eg smart metering); commercial (eg shopping systems); and smart cities (eg smart homes or smart buildings). Figure 1 presents this range. Although this list is not exhaustive, it shows the plethora of opportunities presented by IoT.

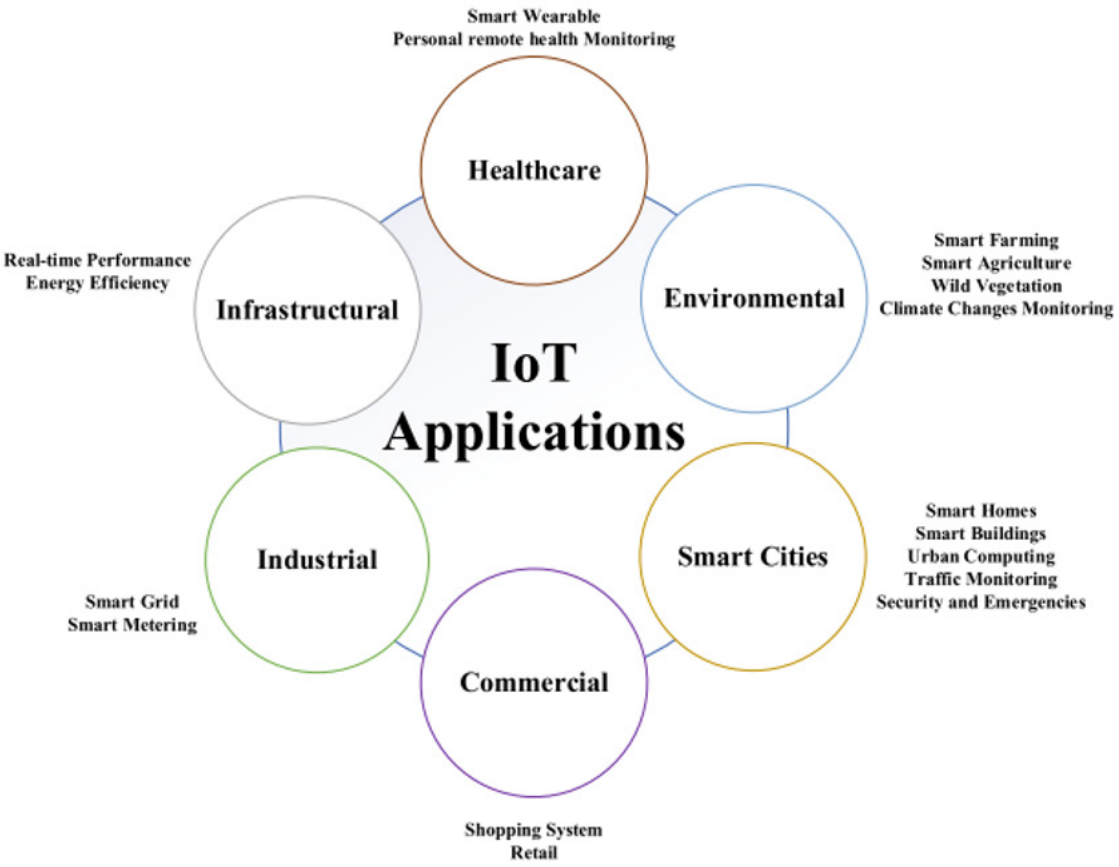


FIGURE 1: IOT APPLICATIONS ADOPTED FROM HASSAN ET AL. (2020: 28)

Turning to the policy implications, Taylor et al. (2018) group IoT applications into three main categories: industrial, public space, and consumer. The authors argue that these three categories have different stakeholders, public expectations, legal contexts, and government requirements (ibid.: 6).

IoT in the home and workplace falls into the categories of public space and consumer. Although distinctions between home and the workplace are very blurred, especially after many people adopted working from home because of the Covid-19 pandemic, there are still boundaries between the way we interact with IoT in a professional capacity and in a personal "home" capacity.

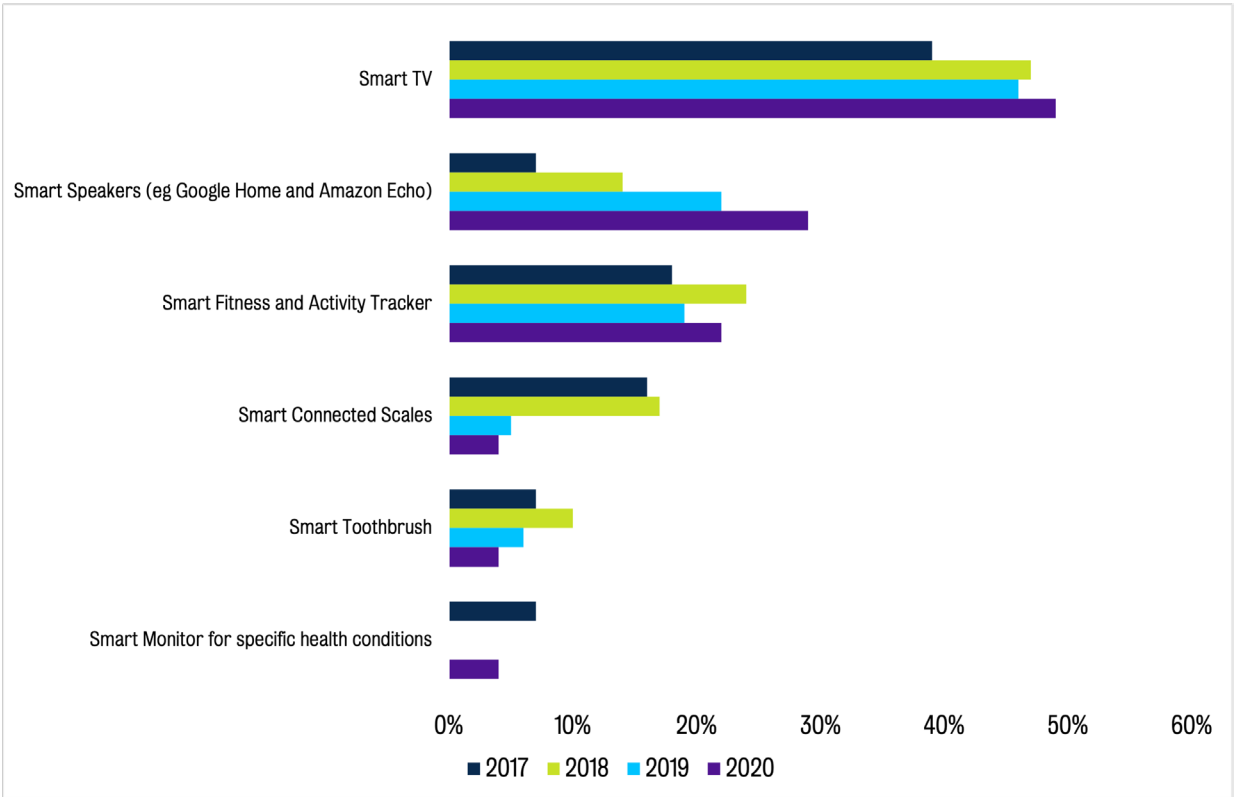
IoT at home

Within the smart home, some examples of IoT devices are smart metering, smart fridges, lighting, robot vacuums, laptops, smartphones and tablets. There are also various IoT services, such as Amazon Echo, Google Home and Nest. These "things" are aimed to assist our daily activities, and with advancements in AI and robotics, it is projected that they will be able to learn and anticipate our needs.

Austin (2019) presented the futurist vision of what IoT could do at our home. You might get woken up earlier than usual by an alarm clock, which scanned your schedule and learned that you have an important presentation. You come back home from work to discover that a package delivered by a drone is waiting for you because health sensors predicted illness and ordered medicine automatically.

Currently, in the UK, the most used smart devices are light bulbs, speakers connected to a voice-controlled device (eg Amazon Echo), and connected temperature sensors at homes (Statista, n.d.). TechUk (2020), in conjunction with GjK, observed that in 2020, there was an increase in smart TV, smart speakers, and smart fitness device ownership compared to previous years in the UK (See Figure 2).

FIGURE 2: SMART HOME PRODUCT OWNERSHIP ADOPTED FROM TECHUK, 2020



Ipsos MORI was commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to conduct research on consumer attitudes towards smart devices. The survey of 2,001 people was conducted between October and November 2020. The report found that "since the start of the coronavirus pandemic in the UK in March 2020, six in ten consumers in the UK (57%) report an increase in their household use of smart devices" (Stannard, et al. 2020: 12).

The stage development of autonomous systems for use in the home is at early stages in the context of IoT. The most used smart devices still require user input, such as voice control to change lighting or managing devices via smartphones.

IoT in the workplace

The list of possible applications of IoT in the workplace is significant. Based on the academic literature review conducted by Nappi & de Campos Ribeiro (2020), the implementation of IoT in the workplace can be divided into workplace effectiveness and employee productivity.

Some of the examples of the current use of IoT in the workplace to enhance workplace activities are: personalised workspace based on sensor data – eg employees can choose a work area based on preferences in terms of natural light or real-time occupancy data; sensors on resources – eg employees can have easier access to room bookings based on availability and proximity and they can view available hot desks; on-demand estates – companies with flexible work policies can analyse the demand for hot desks and decide when and in which areas the office should be closed to save energy and personnel costs (Institute of Workplace and Facilities Management, 2018: 2-4).

In terms of employee productivity, IoT technology (eg wearable sensors) can collect and assess employees' behaviour "to estimate employees' emotional states associated with productivity measures" (Nappi & de Campos Ribeiro, 2020: 79-80). For example, employees' health data can be analysed to design wellness programs to increase productivity (Gaur, Shukla & Verma, 2019: 557). People analytics is another term used where IoT is utilised for improving HR processes and employee productivity (Gaur, Shukla & Verma, 2019).

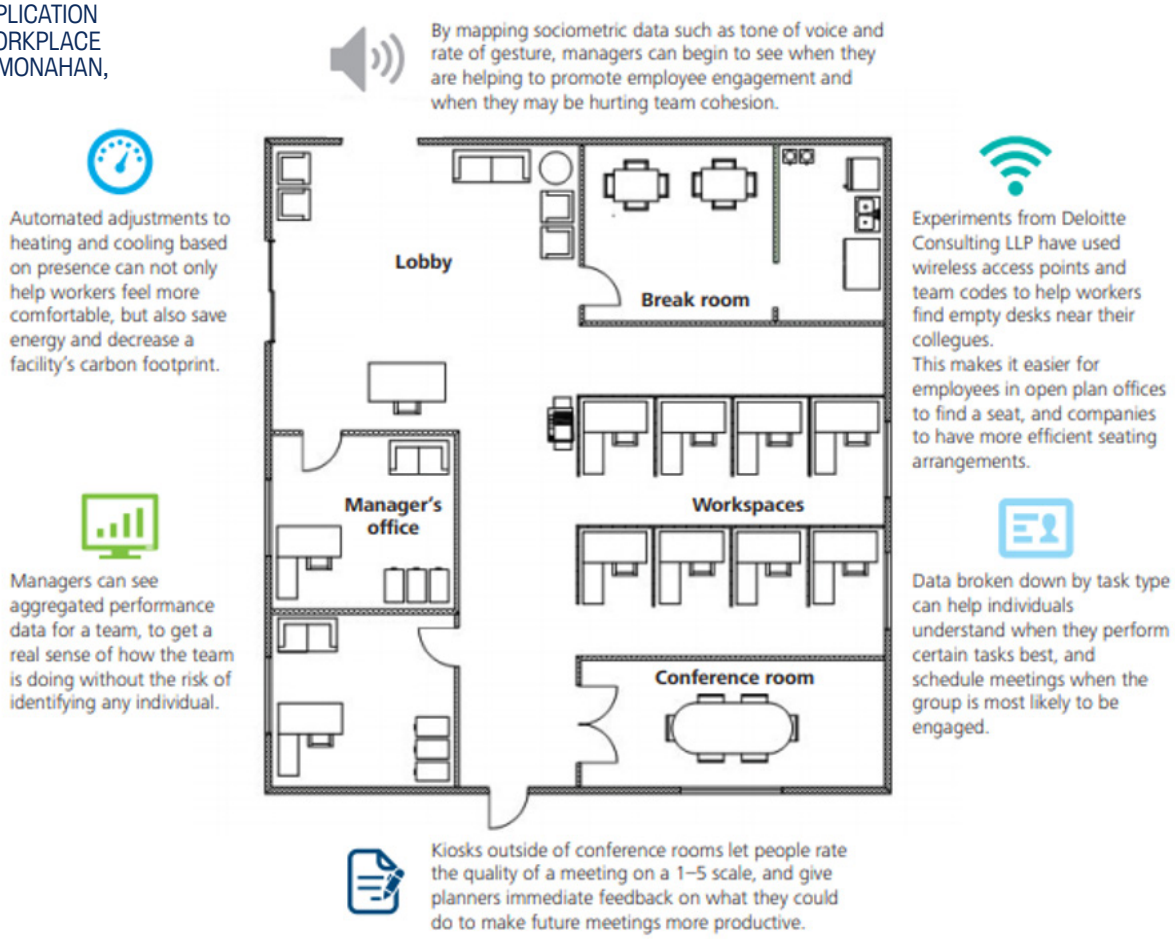
However, using human characteristics for measurement and automation also poses questions over a right to human dignity (Wiewiorowski, 2019), is a challenging topic from an ethical point of view, and has possible unintended consequences.

Mariani & Monahan (2016: 8) provided examples (below) of the use of IoT in the workplace that considers workplace effectiveness and employee productivity. IoT can help with, for example, effective office space planning, and collecting sociometric data to help managers promote employee engagement and team cohesion (see Figure 3).

As can be seen in the figure below, some of these applications raise serious privacy concerns – such as recording voices and gestures of employees – while other examples are less invasive – eg helping workers to find an empty desk. Some other use

examples are, in turn, perhaps questionable in terms of functionality – eg kiosks to rate meetings.

FIGURE 3: APPLICATION OF IOT AT WORKPLACE (MARIANI & MONAHAN, 2016: 8)



The UK policy landscape

The UK has an active interest in the fourth industrial evolution, as can be observed in many policy documents that aim to position the UK at the forefront of new technologies and unlock the potential of these technologies in boosting the economy and creating new jobs.

In 2017, Lynne McGregor (Innovation Lead in the Innovate UK) said that Britain:

> *"Was the birthplace of the first industrial revolution, led the second technological industrial revolution, was an early adopter of the third automation-driven industrial revolution, and is now readying itself to adopt and adapt to the fourth industrial revolution – driven by digital data, connectivity and cyber systems."*

The government set grand challenges for the fourth revolution (BEIS, 2017). These challenges are **artificial intelligence and data economy**, an **ageing society**, **clean growth** and **future of mobility** (BEIS, 2017: 10). The most applicable grand challenge to IoT is in relation to **artificial intelligence and data**. The Department for Digital, Culture, Media & Sport (DCMS) issued the *UK Digital Strategy* in 2017 – some of the points mentioned in this strategy are:

- building a world-class digital infrastructure for the UK
- giving everyone access to the digital skills they need
- making the UK the best place to start and grow a digital business
- creating a safe and secure cyberspace and unlocking the power of data in the UK economy.

(DCMS, 2017)

Digital Secretary, Oliver Dowden, revealed ten tech priorities in 2021 (DCMS et al., 2021). These build on the *UK Digital Strategy 2017* with a few additions, such as levelling up digital prosperity across the UK, using digital innovation to reach Net Zero, and leading the global conversation on tech. On 1 July 2021, the *UK Innovation Strategy* (BEIS, 2021) was also published, which is aligned with some of the priorities set out in the *UK Digital Strategy 2017* and ten tech priorities. More recently, the UK government released its *National AI Strategy* (HM Government, 2021).

Despite these developments, there is a lack of clear strategy from the UK government towards IoT. The exception is the new proposed legislation based on the consultation on security for consumer IoT, where three security requirements for the IoT are suggested:

- All consumer internet-connected device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of consumer IoT devices must provide a public point of contact so anyone can report a vulnerability and it will be acted on in a timely manner.
- Manufacturers of consumer IoT devices must explicitly state the minimum length of time for which the device will receive security updates at the point of sale, either in-store or online"

(DCMS et al. 2020).

This new law is being developed after it was found that many manufacturers had ignored the voluntary Code of Practice for Consumer IOT Security, and 90 per cent of UK consumer manufacturers did not follow vulnerability disclosure (DCMS, 2020).

Aside from this, we can also refer to the world's leading consumer IoT security standard, ETSI EN 303 645 (ETSI, 2021). There is also some other general regulation being developed outside the UK, such as The European Commission's Artificial Intelligence Act – the "AI Act".

The AI Act proposes a risk-manged approach to AI applications based on four categories: unacceptable systems, high-risk systems, and low AI systems or minimal risk systems. This act is likely to impact UK businesses that want to operate in European countries (European Commission, 2021).

Key policy issues

While the IoT brings many opportunities and benefits, it also poses risks that might require further attention or action from the government or from researchers. In this section, the key policy issues arising from the introduction IoT at home and in the workplace are described, with a reflection on policy applicability and suggestions for future research. It must be pointed out, however, similar policy landscapes have been conducted to date (eg Dutton, 2014; Taylor et al., 2018; Tanczer et al., 2019), but these were not focused on specific domains of application of IoT. We also revisit some of the concerns that are relevant to policymakers and linked with their set priorities (eg Net Zero target or levelling up agenda).

Reducing carbon emissions

Despite substantial economic disruptions caused by the global Covid pandemic, the UK government remained committed to achieving a Net Zero goal, as can be seen in the updated *UK Innovation Strategy: Grand Challenges*. One of its missions is to reduce energy consumption in new buildings through innovative solutions and the use of smart technologies (BEIS, 2021).

In response to a consultation on the Future Home Standard, the government suggested plans for newly built buildings to use low carbon heating and be zero-carbon ready by 2025 (Ministry of Housing, Communities and Local Government, 2021). Therefore, it is very likely we will see different, innovative approaches to making new builds more energy-efficient and companies utilising digital, smart products.

Smart meters and thermostats, which help bring energy costs down, are already used in homes and offices. In March 2021, there were 24.2 million smart and advanced meters in homes and small businesses in Great Britain (BEIS, 2021a). These devices are specifically designed to save energy costs, they are purchased (or installed for free) by environmentally friendly customers or those who simply want to save on bills. Although these can be seen as a quick win for the government's Net Zero emissions drive and commitment to building new energy-efficient homes and offices, it is not clear that they actually have a positive environmental impact, especially when it comes to their production, transportation and recycling (see, eg Louis et al. 2015; Aleksic & Mujan, 2016).

Moreover, smart things are not just used to make homes and offices more energy efficient. For example, we also have devices such as smart fridges, robotic vacuum cleaners, and security cameras, where the primay goal has nothing to do with saving energy costs. What is more, as Finely (2014) observed, it is difficult for customers to be aware of the actual environmental impact of these products as there are not enough certification and standards to provide comprehensive information. Users might be aware of how energy efficient a product is, but they will not know the energy costs of producing it, and companies that use many different components from different manufacturers might not possess this information either.

Stead et al. (2020: 2) also notice an increase in datafication (the production, processing and storage of users' data and automated data). We currently produce around 16 zettabytes of data globally every year (Goodbody, 2018). This number

could increase to 160 zettabytes by 2025 (ibid.) and be accelerated by technological developments, such as the use of 5G networks (Kenworthy, 2019).

Stead et al. (2020) flagged that practitioners should consider the environmental impact of smart devices, and comment that, just because something can be developed from a technological point of view, it does not necessarily mean it should be. The authors also suggest Edge Computing (EC) optimisation as a solution, whereby data are processed closer to its origin rather than transmitting to central data warehouses. This may be more environmentally sustainable, especially when it comes to minimising data distribution. However, EC optimisation decisions must be carefully thought through because not all tasks executed by devices in an IoT environment can be offloaded this way. Other factors, such as wireless network state, device capabilities, and privacy and security issues must also be taken into account (Sadatdiynov, 2022).

There is also an issue with smart devices' longevity and disposal. From a business perspective, companies want customers to buy new versions of their products, but many older models will end up in landfills, creating more waste and potentially releasing hazardous emissions into the environment (Finely, 2014; Gurova, 2020).

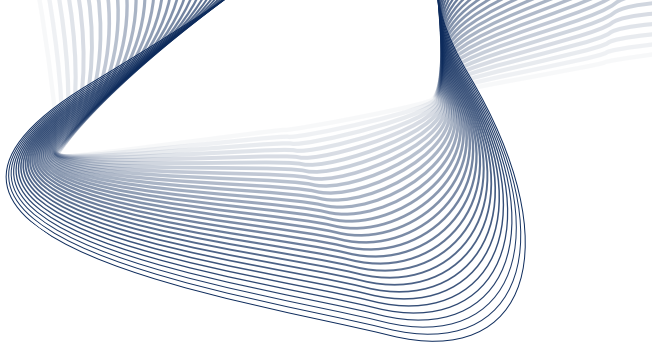
One solution is to encourage customers to repair and exchange parts, but this approach requires companies to be incentivised to develop business models that allow for their pieces to be easily disassembled and repaired while minimising the environmental impact (Gurova, 2020). Additionally, with electronic device disposal, there is a risk that data that were collected for a different purpose will end up being used by third parties who resell components (Schafer, 2015)

The government is active in enabling and promoting the rollout of smart meters (Ofgem, n.d.), but it also needs to work with academia and industry to understand how existing and new smart things will help in delivering its climate goals. There have already been some attempts to encourage digital technologies companies to reduce the environmental impact within manufacturing processes (eg by providing £20 million funding for businesses to apply for), but the government might need to do more than this, such as develop policies and standards to ensure the sustainability of IoT during its life-cycle, and consider data protection regimes of recycled items. Without careful consideration by the government, IoT can negatively impact the environment, despite its promising potential in improving energy usage.

Security issues

As the IoT connects the internet, there are potential security risks. Although security challenges are not new in the IT sector, as Tawalbeh et al. (2020: 4) noted, IoT raises new security issues that need to be addressed.

IoT is not just technology – it is a complex social-technical system, impacting online, offline realms as well as humans (Taylor et al., 2018: 31). The OECD (2016: 18) issued a recommendation for digital security risk management, suggesting that policymakers and leaders should not view security issues as only technical problems, but also as economic and social dangers. For example, if a building is controlled by a



smart door and locks and gets hacked by a malicious user, its security and personnel will be compromised (Figliola, 2020). The damage might also include loss of data. This can negatively impact the company's reputation, cause loss of important information, affect market position (eg through theft of innovation), and disrupt the company's operations (OECD, 2016: 20).

This is one example of what can happen when poor security choices are made. The IoT is very often designed to use low memory and energy, ipso facto limiting its security solutions (Strous, et al. 2021 & Ogonji et al. 2020). Companies developing IoT devices – which are designed from the beginning to be disposable – might not have enough experience to provide adequate security solutions (FTC, 2015). In fact, the manufacturers did not build important security requirements, which resulted in introducing legislation on IoT security requirements, as discussed in the previous section (DCMS et al. 2020).

This legislation is seen as a good step towards ensuring the safety of IoT products, but the government might need to think further in terms of product liabilities in case of data or security breaches – for example, who will be responsible when technology makes mistakes or behaves in unintended ways? Innovative research and suggested solutions to protect customers' privacy and enhance security in domestic settings can raise legal issues. According to Chen et al. (2020) the existing regulatory framework, the General Data Protection (GDPR) – which is retained in domestic law as the UK GDPR and kept under review – does not adequately address issues of accountability, and it may even place disproportionate regulatory burdens on developers, users and contributors.

In academia, researchers have developed different solutions to mitigate security risks (Ogonji et al. 2020) by mainly focusing on technical perspectives, such as increasing the update frequency or deployment of monitoring device tools (Tawalbeh et al. 2020). But, as Ogonji et al. (2020) noted, many researchers failed to recognise the need for a user-centric approach when designing and implementing IoT devices.

The user-centric design puts a user at the centre of device design by focusing on their needs and requirements (Krajewski, 2017). The user-centricity approach also enables users to be in charge of "their own information and contextual integrity", ipso facto merging the IoT into people's everyday lives (Ogonji et al., 2020: 4), demonstrating a gradual shift in the technical community towards thinking about the IoT and its relationship with people. However, the user-centric design will require some basic knowledge and skills from the user to understand why certain input is needed and what it does. This itself puts a stronger responsibility on technology designers to think about how IoT will be used in practice and anticipate how design features will impact user experience.

Data, privacy and ethical issues

Security and privacy of IoT are very often discussed together. They are crucial factors in ensuring safety and trust in smart things. As an autonomous object in IoT is capable of collecting users' information without their awareness, IoT devices raise ethical questions too. On the one hand, increased data availability can lead to more

innovation, and enhancement of products and services, but at the same time, it raises serious concerns over privacy and data exploitation. Information about an individual collected through a smart object can be used to monitor their habits, daily routines, and location, as well as activities at work. Because IoT very often has sensors and cameras, they can also lead to the invasion of privacy if they are hacked.

Issues associated with privacy and ethical issues at home

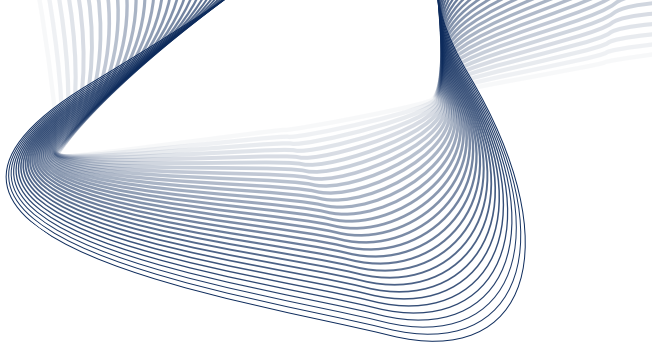
At home, we can already see examples of smart things and concerns over the personal data they collect and how these data are used. For example, Alexa is a voice assistant speaker that technically should only listen to the user's commands when the wake-up word is used. However, as Chokshi (2018) observes, Alexa, by its design is listening to people's conversations all the time; otherwise, it would not know when the wake-up word was used. What is more, there are many reported cases highlighting the potential invasion of privacy that devices like Alexa can pose. For example, numerous instances when Alexa misheard the wake-up word (Lynskey, 2019), a case where an individual's data were requested by a judge to be used to solve a murder (Cuthbertson, 2018), and instances of voice recordings be sent to the wrong people (Griffin, 2018).

Although Alexa should only record what is being said after the wake-up word is triggered, these examples show that technology can make mistakes and act in ways other than its intended purpose, and that its data can be used for other purposes than intended. For IoT to be trusted, user privacy needs to be safeguarded and data be collected and used for agreed purposes and in an ethical manner.

Amazon has recently added some features to its Alexa devices, such as allowing users to delete recorded data or mute a microphone. Cho et al (2020) found that customisable privacy settings in their developed app for Amazon Alexa had a positive effect in enhancing trust and usability in regular users, but it provided the opposite result in power users (people who show traits toward being more efficient and competent in using new technologies). Power users reported higher trust towards Alexa, but only in the absence of privacy customisation. While for users who expressed great concerns about privacy, trust in the device is the highest when they are presented with the option of customising privacy and content settings.

Although this study shows some indication of how trust in Alexa devices can be increased through design, it does not entirely solve the problem with privacy concerns. First of all, users need to be aware of different functions to protect their privacy. We do not know how many Alexa or other smart device users are aware of privacy risks and what features they can use to manage their data and privacy.

Secondly, research on online behaviour has shown a discrepancy in users' beliefs towards privacy and their actual behaviour (Gerber et al., 2018). Users can claim to be very concerned about privacy, but take very few steps to protect it and not read details about their data use before giving consent (Muravyeva et al. 2020 cited in Elsen et al. 2014). This phenomenon is referred to as the privacy paradox. It poses a challenge for policymakers in deciding whether privacy choices should be imposed through legislation when users voluntarily disclose their information (Norberg et al., 2007).



Because the behaviour of users towards privacy is a complex topic and most studies are set in a specific context, we recommend that the government works with diverse stakeholders – eg researchers from different disciplines and the private sector – to find the best solutions. More work is also required to establish whether companies provide enough information for customers to know how their personal data are used. As Noto La Diega & Sappa (2020) note, customers might not be aware of how their personal data are utilised due to technical – the opacity of the algorithms – and legal – a combination of trade secrets and strategic contract management – secrecy.

Issues associated with privacy and ethical issues in the workplace

In the workplace, IoT and privacy risks are mainly associated with the employer monitoring of employee activity. Although analysing worker performance is not a new phenomenon, and it has been practised for a long time, smart devices bring possibilities of collecting data about an employee that were not previously possible, such as socio-metrics about their tone and voice (Mariani & Monaha, 2016). The pandemic had also brought new challenges towards surveillance of worker performance and privacy when many people moved to work from home or hybrid working, blurring the lines between private and work environments.

The BBC (2021) reported that 32 per cent of home workers are monitored using some mechanism of online surveillance, based on a survey conducted by Opinium for the trade union Prospect. Furthermore, the findings from the survey show that people aged 18-34 years old are more likely to be monitored (48 per cent) than other colleagues (BBC, 2021). Camera or different software applications for tracking employees are currently mainly adopted for home workers (ibid.). However, new ways of monitoring by using IoT systems are likely to appear with flexible and hybrid working options becoming more popular.

The UK's data protection authority, the Information Commissioner's Office (ICO) provides The Employment Practice Code with a section on monitoring (ICO, n.d.). The guidance suggests that monitoring activities need to be compliant with Data Protection Act; however, it does not reflect new methods of workers' surveillance at home. According to Azer (2021), policymakers and researchers should investigate this subject more.

The research so far has focused on studying productivity in terms of workplace surveillance, but less attention has been given to data justice, which means fairness in the way people are made visible, represented and treated as a result of their production of digital data (Azer, 2021; Tylor, 2017). The exception is the study by Ball (2021) on mitigating the psycho-social risks of monitoring, which draws on privacy, data justice and organisational justice principles and makes numerous recommendations both for practice and for higher level policy development.

The government has launched a consultation, *Data: a new direction*, which closed in September 2021. One of its sections was devoted to data fairness in AI. The government, in its consultation, recognised that there is a close interrelationship between fairness, bias and discrimination, and sought views on, among other things, whether current legal obligations with regards to fairness are clear when developing and/or deploying AI systems.

Skills and jobs

The impact of technological developments on jobs and skills is not new, and it has also been discussed in our previous policy landscapes reviews (see eg Lisinska, 2021). In the Blackett review on IoT from 2014, one of the observations was that people would require a new set of skills to design, develop, and maintain smart devices (Government Office for Science, 2014). Since then, the government has published its ten year national strategy on AI, with plans to develop skills and attract the best talent when developing AI systems. One of its immediate plans is to support the development of AI, data science, and digital skills through the Department for Education's Skills Bootcamps (HM Government, 2021).

However, these plans are not directly aimed at supporting workers whose tasks become displaced by IoT systems and more automation in the workplace. The workers who lose their jobs are unlikely to benefit from new jobs that are being created, considering the pace of technological developments and the new skills that will potentially be required (eg Oppenheimer, 2019).

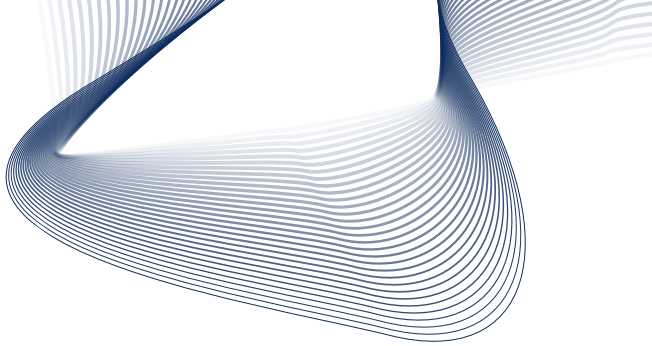
PwC has recently conducted a study looking at how AI and related technologies impact on jobs for the Department for Business, Energy and Industrial Strategy (BEIS). The study finds that managerial and professional occupations will likely see net employment benefits. At the same time, clerical and manual workers are more likely to see a negative net employment impact over the next 5-10 years. Net employment benefits may be more visible in London and the South East than in the Midlands and North England (BEIS Research Report, 2021).

Although this study shows some estimations, and more research is needed, we suggest that the government starts developing clear policies in upskilling and reskilling the existing workforce. As technological advancement may widen existing geographical inequalities over time, implementing the levelling up agenda will not happen without significant government intervention.

Skills that will become essential when using IoT must be also taken seriously into consideration by the government. This is not to only ensure that IoT systems are used in proper ways – eg users are able to set secure passwords for the safe operation of IoT, and know how to set up privacy settings – but also so all people have equal opportunities in using smart devices and can gain maximum benefits.

The government has defined the Essential Digital Skills (EDS) framework for life based on five categories that an individual should have:

- **Communicating:** the skills required to communicate, collaborate and share information.
- **Handling information and content:** the skills required to manage and store digital information and content securely.
- **Transacting:** the skills required to register and apply for services, buy and sell goods and services, and manage transactions online.



- **Problem-solving:** the necessary skills to find solutions to problems using digital tools and online services.
- **Being safe and legal online:** The skills required to stay safe, legal and confident online.

The Lloyds Bank Consumer Digital Index conducts an annual study of UK digital skills, including measurement of skills against the EDS framework. The *Essential Digital Skills Report 2021* shows that c.10 million (19 per cent) of UK adults do not have fundamental digital skills, and c. 2.8 million people (6 per cent) cannot do any of the foundational digital tasks.

To have the foundations of essential digital skills, an individual must perform seven tasks in total – for example, be able to use a device, connect to a Wi-Fi network and create and update passwords. Only 28 per cent of people aged 75+ have these foundation-level skills. The study concluded that an estimated 10 million people are digitally excluded and at risk of online harm when they decide to use online tools (Lloyds Bank, 2021). Even though this report does not focus on digital skills when engaging with smart devices, a similar set of skills is required to use IoT successfully.

In the previous section (see: Security), we note a movement towards a user-centric approach to security and privacy, where the user is in control. However, this requires proper skills so users can change and update their contextual integrity when using smart devices and understand why certain input is needed from them, what information is being collected, and the risks associated with disclosing certain data about themselves.

Conclusion

In this policy review, we have sought to scope key policy issues arising from IoT use. The potential application of IoT is enormous, but we focused on two domains, IoT at home and in the workplace. However, some of the issues disussed can be applied to the whole IoT ecosystem. Although IoT is growing exponentially, its growth might slow down slightly in the coming years due to the global chip shortage. This situation provides policymakers and researchers with opportunities to revisit and address some issues now.

First of all, IoT is not just a technical object but a complex socio-technical system. This means that researchers need to work across different disciplines to address some of its problems. Technological solutions might not be enough. For example, in terms of privacy, designing customisable privacy settings for users to give them control over their data is not a sufficient fix, especially when we do not know how many people use this feature, how they use it, or even if they are aware of such an option. Besides this, online behaviour research indicates that there can be a disconnect between people's online behaviour and their stated views on privacy.

We also draw attention to the fact that suggested privacy and security issues will require some basic digital skills from users. So far, the government has shown interest in providing the skills necessary for building AI systems, but skills that people need to use IoT in a safe and effective way – eg to manage privacy settings, or be able to set secure passwords for the safe operation of IoT – are not explored. Plans to reskill existing workers whose tasks become displaced by IoT systems are also not visible. We have also identified a clear need for policymakers to work with academia to understand the environmental impact of IoT and how to minimise this in order to achieve the Net Zero target by 2050.

References

Aleksic, S., & Mujan, V. (2016) Exergy-based life cycle assessment of smart meters. *ELEKTRO 2016 - 11th International Conference, Proceedings*, 248–253. https://doi.org/10.1109/ELEKTRO.2016.7512075

Azer, E. (2021) *Remote working has led to managers spying more on staff – here are three ways to curbit*. Available from: https://theconversation.com/remote-working-has-led-to-managers-spying-more-on-staff-here-are-three-ways-to-curb-it-159604. Accessed 07/12/2021.

Ball, K. (2021) *Electronic Monitoring and Surveillance in the Workplace, Publications Office of the European Union*, Luxembourg, 2021, ISBN 978-92-76-43340-8 (online), doi:10.2760/5137 (online), JRC125716.

BBC (2021*) 'The way my boss monitored me at home was creepy'*. Available from: https://www.bbc.com/news/uk-politics-59152864. Accessed 07/12/2021.

BEIS (2021) *The Grand Challenge missions*. Available from: https://www.gov.uk/government/publications/industrial-strategy-the-grand-challenges/missions#buildings. Accessed 01/11/2021.

BEIS (2021a) *Smart Meter Statistics in Great Britain: Quarterly Report to end March 202*1. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/988831/Q1_2021_Smart_Meters_Statistics_Report.pdf. Accessed 01/11/2021.

BEIS et al (2021) *UK enshrines new target in law to slash emissions by 78% by 2035.* Available from: https://www.gov.uk/government/news/uk-enshrines-new-target-in-law-to-slash-emissions-by-78-by-2035. Accessed 01/11/2021.

BEIS Research Report (2021) *The Potential Impact of Artificial Intelligence on UK Employment and the Demand for Skills: A report by PwC for the Department for Business, Energy and Industrial Strategy*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1023590/impact-of-ai-on-jobs.pdf. Accessed 12/12/2021.

Brown, D. (2022) Apple iPhone Users Got Alerts About Strangers' AirTags. The Trackers Were Never Found. Available from: https://www.wsj.com/amp/articles/phantom-airtag-alerts-send-iphone-users-on-wild-goose-chases-11651799060?utm_campaign=The%20Week%20in%20Data%20TWID&utm_medium=email&utm_content=213010536&utm_source=hs_email. Accessed: 15/5/2022

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*, Volume 10, Issue 4, November 2020, Pages 279–293, https://doi.org/10.1093/idpl/ipaa011

Cho, E. S. et al. (2020) Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customisation on User Experience of Smart Speakers. *In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. DOI:https://doi.org/10.1145/3313831.3376551

Chokshi, N. (2018) Is Alexa listening?: Amazon echo sent out recording of couple's conversation. *New York Times*. 25th May. Available at https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html. Accessed 01/11/2021

Congressional Research Service (2020) *The Internet of Things (IoT): An overview*. Available from: https://crsreports.congress.gov/product/pdf/IF/IF11239. Accessed 01/11/2021

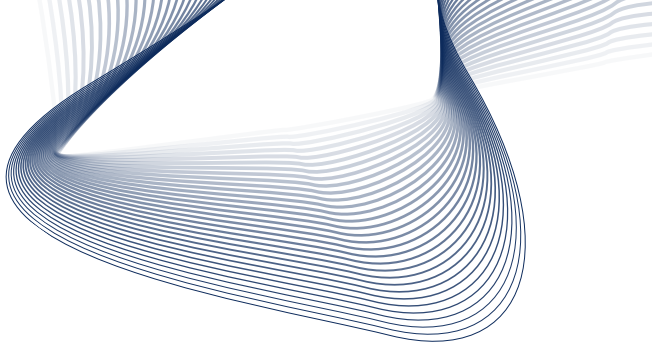
Cuthbertson, A. (2018) Amazon ordered to give Alexa evidence in double murder case. *The Independent*,14th Nov. Available from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-echo-alexa-evidence-murder-case-a8633551.html. Accessed 01/11/2021

Currall, S., et al. (2006) What drives public acceptance of nanotechnology?. *Nature Nanotech* 1, 153–155. DOI: https://doi.org/10.1038/nnano.2006.155

DCMS (2019) *ETSI industry standard based on the Code of Practice*. Available from:
https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-code-of-practice. Accessed 14/01/2021.

DCMS (2020) *Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.* Available from: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation. Accessed 02/08/2021.

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.



DCMS *et al*. (2021) *New strategy to unleash the transformational power of Artificial Intelligence*. Available from: https://www.gov.uk/government/news/new-strategy-to-unleash-the-transformational-power-of-artificial-intelligence. Accessed 02/08/2021.

Department for Business, Energy and Industrial Strategy (2017) *Industrial strategy: building a Britain fit for the future*. Available from: www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future. Accessed 02/08/2021.

Department for Business, Energy and Industrial Strategy (2017). *Made Smarter*. Available from: www.gov.uk/government/publications/made-smarter-review. Accessed 02/08/2021.

Department for Business, Energy and Industrial Strategy (2019) *Regulation for the Fourth Industrial Revolution*. Available from: https://www.gov.uk/government/publications/regulation-for-the-fourth-industrial-revolution. Accessed 02/08/2021.

Department for Digital, Culture, Media and Sport (2019) *Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation*. Available from: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation. Accessed 02/08/2021.

Department for Digital, Culture, Media and Sport and The Rt Hon Karen Bradley MP (2017) *UK Digital Strategy*. Available from: www.gov.uk/government/publications/uk-digital-strategy. Accessed 02/08/2021.

Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the Internet of things. *Info*, *16*(3), 1–21. https://doi.org/10.1108/info-09-2013-0047.

Dutton, W.H. (1999) *Society on the Line*. Oxford University Press. Oxford

Edquist, H., Goodridge, P., & Haskel, J. (2021). The Internet of Things and economic growth in a panel of countries. *Economics of Innovation and New Technology*, 30(3), 262–283. https://doi.org/10.1080/10438599.2019.1695941.

ETSI (2021) ERSI releases test specification to comply with world-leading consumer iot security standard. Available from: https://www.etsi.org/newsroom/press-releases/1983-2021-10-etsi-releases-test-specification-

to-comply-with-world-leading-consumer-iot-security-standard. Accessed 9/03/2022.

European Commission (2021) *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Brussels: European Union. Available from: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Accessed 9/03/2022.

Figliola, P. (2020) The Internet of Things (IoT): An Overview. Congressional Research Service. Available from: https://crsreports.congress.gov. Accessed 02/08/2021.

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

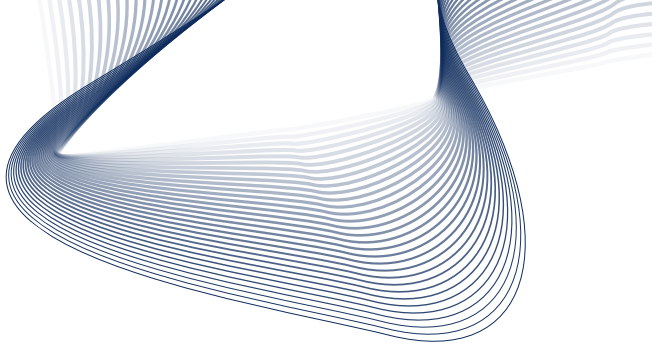
FTC (2015) *Internet of Things: Privacy and Security in the Connected World*. Available from: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Accessed 21/03/2022.

Garcia-Morchon, et al. (2019) Oscar Garcia-Morchon, Sandeep Kumar, Mohit Sethi,
Internet of Things (IoT) Security: State of the Art and Challenges. Available from: https://datatracker.ietf.org/doc/rfc8576/. Accessed 13/01/2022.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behaviour. *Computers and Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Goodbody, W. (2018). Waterford Researchers Develop New Method To Store Data In DNA. Available from: https://tinyurl.com/y7g4g4fp. Accessed 12/03/2022.

Government Office for Science (2014) *Internet of things: making the most of the second digital revolution*. Available from: https://assets.publishing.service.gov.



uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf. Accessed 25/06/2021. Accessed 28/06/2021.

Government Office for Science (2014) *Internet of things: making the most of the second digital revolution*. Available from: www.gov.uk/government/publications/internet-of-things-blackett-review. Accessed 02/08/2021

Gregersen, C. R. (2021) *How the Worldwide Chip Shortage Affects IoT*. Available from: https://dzone.com/articles/how-the-worldwide-chip-shortage-affects-iot. Accessed 01/01/2021.

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

GSMA Wireless Intelligence Database. Accessed July 23, 2021. www.gsmaintelligence.com. GSMA

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

HM Government (2021) *National AI Strategy*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf Accessed 02/08/2021.

Höller, J. et al. (2014) *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Amsterdam: Elsevier Science.

ICO (n.d.) *The employment practices code*. Available from: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf. Accessed 07/12/2021.

Institute of Workplace and Facilities Management (2018) *Internet of Things for facility management services. An overview of the impact of IoT technologies on the FM services sector*. Available from: https://www.iwfm.org.uk/uploads/assets/4ee0fcb7-d0ad-4f75-a61e491cc91db0da/Internet-of-things.pdf. Accessed 02/08/2021.

Intertrust Technologies (2017) *How Do You Ensure Trust in IoT?* Available from: https://medium.com/iotforall/human-centric-trust-model-for-iot-a98c04fceec1/ Accessed 11/01/2021.

ISOC-OTA (2018) The Internet Society, "Online Trust Alliance (OTA)" *Internet of Things (IoT) Trust Framework v2.5*. Available from: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/. Accessed 13/01/2022.

Kenworthy, R. (2019) *The 5G And IoT Revolution Is Coming: Here's What To Expect*. Available from: https://tinyurl.com/voyut7s. Assessed 9/03/2022.

Krajewski, A. (2017) *User Centred IoT Design*. Available from: https://medium.com/the-state-of-responsible-internet-of-things-iot/andreakrajewski-aff52af1e065. Accessed 03/11/2021.

Kramp T., van Kranenburg R., Lange S. (2013) Introduction to the Internet of Things. In: Bassi A. et al. (eds) *Enabling Things to Talk*. Springer, Berlin, Heidelberg.DOI: https://doi.org/10.1007/978-3-642-40403-0_1

Lisinska, J. (2021) Autonomous vehicles on public roads in maritime and aerial – a policy landscape review. DOI: https://doi.org/10.18742/pub01-064

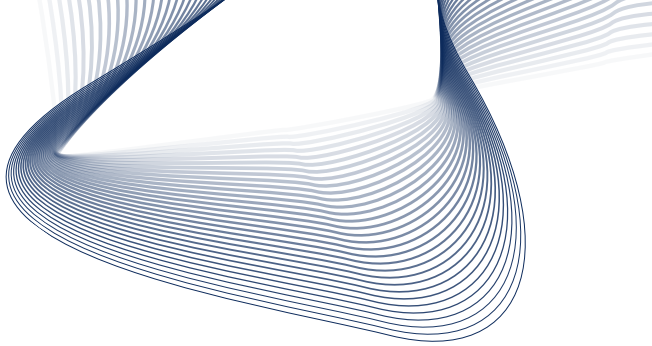
Lloyds Bank (2021) *Essential Digital Skills Report 2021*. Available from: https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/211109-lloyds-essential-digital-skills-report-2021.pdf. Accessed 11/12/2021.

Louis, J. N., Caló, A., Leiviskä, K., & Pongrácz, E. (2015) Environmental impacts and benefits of smart home automation: Life cycle assessment of Home Energy Management System. *IFAC-PapersOnLine*, *28*(1), 880–885. https://doi.org/10.1016/j.ifacol.2015.05.158

Lynskey, D. (2019) 'Alexa, are you invading my privacy?' – the dark side of our voice assistants. *The Guardian*, 9th Oct. Available from: https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants. Accessed 01/11/2021

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

Mariani, J., & Monahan, K. (2016) Will IoT technology bring us the



quantified employee? The Internet of Things in human resources. *Deloitte University Pres*, 1–20. Available from: http://www2.deloitte.com/us/en/pages/tech-nology-media-and-telecommunications/topics/the-internet-of-things.html Accessed 02/08/2021.

McGregor, L. (2017) What does the fourth industrial revolution (4IR) mean for UK business? Innovate UK. *28th March*. Available from: https://innovateuk.blog.gov.uk/2017/03/28/what-does-the-fourth-industrial-revolution-4ir-mean-for-uk-business/. Accessed 02/08/2021.

Minerva R., Biru A., Rotondi D. (2015) *Towards a Definition of the Internet of Things (IoT)*. IEEE Internet Initiative. Available from: iot.ieee.org. Accessed 28/06/2021.

Ministry of Housing, Communities and Local Government (2021) *Government response to Future Home Standard*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/956094/Government_response_to_Future_Homes_Standard_consultation.pdf Accessed 01/11/2021

Motlagh, N. H., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020) Internet of things (IoT) and the energy sector. *Energies*, *13*(2), 1–27. https://doi.org/10.3390/en13020494

Nappi, I., & de Campos Ribeiro, G. (2020) Internet of Things technology applications in the workplace environment: a critical review. *Journal of Corporate Real Estate*, *22*(1), 71–90. https://doi.org/10.1108/JCRE-06-2019-0028

Noto La Diega, G. and Sappa, C. (2020) The Internet of Things at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Appropriation and Empower Consumers. *Revue européenne de droit de la consommation / European Journal of Consumer Law*, pp. 419-458. DOI: SSRN: https://ssrn.com/abstract=3772700

Norberg P. A., Horne D. R., and Horne D.A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs. V*ol. 41 (1) pp. 100-127

OCED (2016) The Internet of things: seizing benefits and addressing the challenges. 2016 Ministerial meeting on the digital economy. Background report. *OCED publishing*.No. 252

OCED (2018) *IoT measurement and applications. OECD digital economy*

papers. October 2018 No. 271. Available from: https://iotbusinessnews.com/download/white-papers/OECD-IoT-Measurement-Applications.pdf. Accessed 26/07/2021

Ofgem (2017) *Upgrading Our Energy System Smart Systems and Flexibility Plan*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/633442/upgrading-our-energy-system-july-2017.pdf. Accessed 02/08/2021.

Ofgem (n.d.) *Getting a smart meter*. Available from: https://www.ofgem.gov.uk/information-consumers/energy-advice-households/getting-smart-meter. Accessed 01/11/2021.

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020) A survey on privacy and security of Internet of Things. *Computer Science Review*, 38, 100312. https://doi.org/10.1016/j.cosrev.2020.100312

Oppenheimer, A (2019) *The Robots Are Coming: The Future of Jobs in the Age of Automation*, Vintage

Record Evolution (n.d.) *IoT and Sustainability: What Is the Environmental Impact*? Available from: https://www.record-evolution.de/en/iot-and-sustainability-the-environmental-impact-of-the-internet-of-things/. Accessed 01/01/2021.

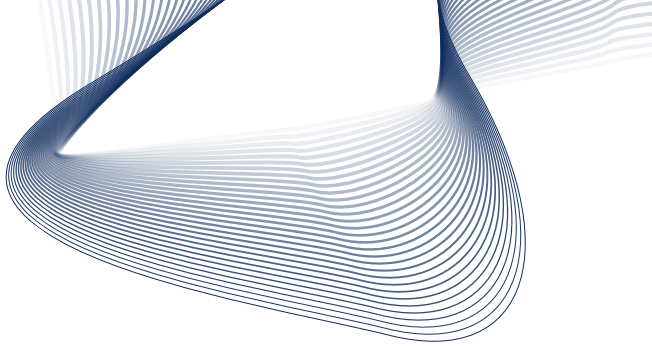
Sadatdiynov, K., Cui, L., Zhang, L., Huang, J. Z., Salloum, S., & Mahmud, M. S. (2022). A review of optimisation methods for computation offloading in edge computing networks. *Digital Communications and Networks*.

Schafer, B. (2015) 'D-waste: Data disposal as challenge for waste management in the Internet of Things'. *International Review for Information Ethics*. Vol. 22(1), pp. 100-106.

Schwab, K. (2016) *The Fourth Industrial Revolution: what it means, how to respond*. Available from: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/. Accessed 02/08/2021.

SAE (2022) *International Taxonomy and Definitions for Terms Related to On-road Motor Vehicle Automated Driving Systems*. Available from: https://www.sae.org/standards/content/j3016_202104. Accessed 02/08/20221.

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018) What is a smart device? - a conceptualisation within the paradigm of the Internet of things.



Visualisation in Engineering, *6*(1). https://doi.org/10.1186/s40327-018-0063-8

Stannard, J., Writer-Davies, R., Spielman, D., & Nurse, J. (2020) *Consumer Attitudes Towards IoT Security Report*. (December), 1–33. Available from: from http://www.ipsos-mori.com/terms.

Statista (n.d.) *Do you own Smart Home devices – i.e. devices that you can control via a smartphone / an internet connection*? Available from: https://www.statista.com/forecasts/997845/smart-home-device-ownership-in-the-uk. Accessed 29/07/2021.

Stead,M. at el (2020) Edge of Tomorrow: Designing Sustainable Edge Computing. n Boess, S., Cheung, M. and Cain, R. (eds.), *Synergy - DRS International Conference 2020*, 11-14 August, Held online. https://doi.org/10.21606/drs.2020.293

Strous, L., von Solms, S., & Zúquete, A. (2021) Security and privacy of the Internet of Things. *Computers and Security*, *102*, 102148. https://doi.org/10.1016/j.cose.2020.102148

TAS-Hub (2020) *Our definitions*. Available from: https://www.tas.ac.uk/our-definitions/. Accessed 27/06/2021.

Tanczer, et al. (2019). *The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape*. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity Governance* (pp. 37–56). Hoboken, New Jersey: Wiley.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020) *Applied sciences IoT Privacy and Security: Challenges and Solutions*. *Mdpi*, 1–17. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020) Applied sciences IoT Privacy and Security: Challenges and Solutions. *Mdpi*, 1–17.

Taylor, L. (2017) What is data justice? The case for connecting digital rights and freedoms globally. *Big Data and Society*, *4*(2), 1–14. https://doi.org/10.1177/2053951717736335

Taylor, P., *et al.* (2018) Internet of Things realising the potential of a trusted smart world. Royal Academy of Engineering: London.

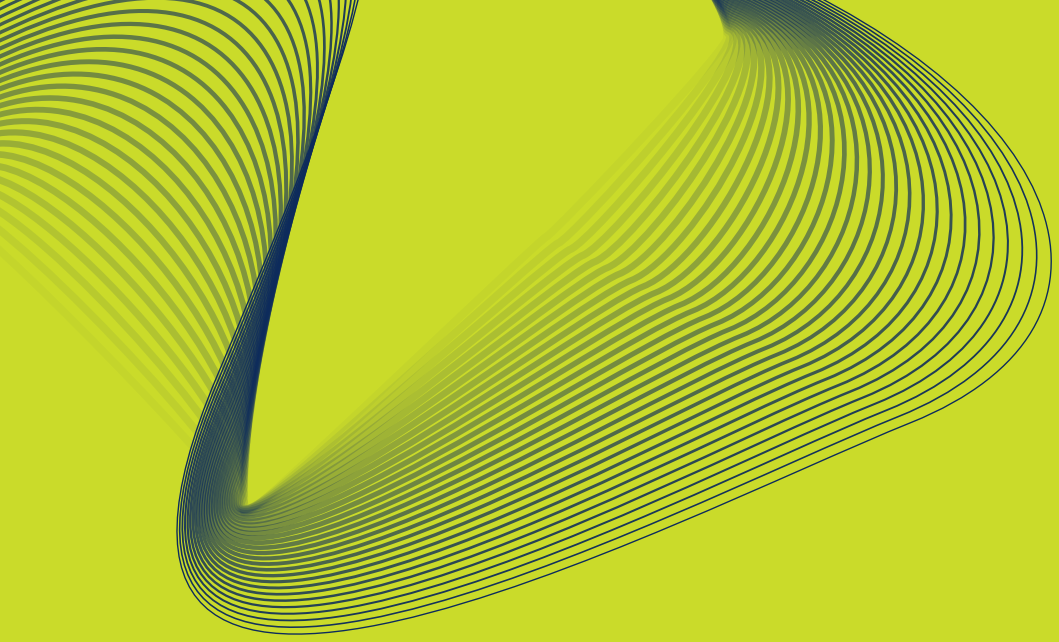
TechUK (2020) *The State of the Connected Home*. Available from: https://spark.adobe.com/page/xAZEUOfDB4I9E/#i-the-connected-home-report-%E2%80%93-overview. Accessed 29/07/2021.

United States Department of Defense (2016) *Policy Recommendations for The Internet of Things (IoT)*. (December), 3–24. Available from: https://www.hsdl.org/?abstract&did=799676. Accessed 28/06/2021.

Voon, J. (2016) *Defining the Internet of things*. Available from: https://innovateuk.blog.gov.uk/2016/04/06/defining-the-internet-of-things/. Accessed 25/06/2021.

Wiewiorowski, W. (2019) *Facial recognition: A solution in search of a problem? European Data Protection Supervisor*. Available at: edps.europa.eu/node/5551 Accessed 30 October 2021.

Winickoff, D. (2017) Public acceptance and emerging production technologies. In: OCED (2017) *The Next Production Revolution Implications for Governments and Business*. https://doi.org/10.1787/9789264271036-en



The Policy Institute

The Policy Institute at King's College London works to solve society's challenges with evidence and expertise.

We combine the rigour of academia with the agility of a consultancy and the connectedness of a think tank.

Our research draws on many disciplines and methods, making use of the skills, expertise and resources of not only the institute, but the university and its wider network too.

Connect with us

@policyatkings kcl.ac.uk/policy-institute