House of Commons

Culture, Media and Sport Committee

Connected tech: smart or sinister?

Tenth Report of Session 2022–23

Report, together with formal minutes relating to the report

Ordered by the House of Commons
to be printed 11 July 2023

HC 157
Published on 7 August 2023
by authority of the House of Commons

The Culture, Media and Sport Committee

The Culture, Media and Sport Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Department for Culture, Media and Sport and its associated public bodies.

Current membership

Dame Caroline Dinenage MP *(Conservative, Gosport)* (Chair)

Kevin Brennan MP (*Labour, Cardiff West*)

Steve Brine MP (*Conservative, Winchester*)

Clive Efford MP (*Labour, Eltham*)

Julie Elliott MP (*Labour, Sunderland Central*)

Damian Green MP (*Conservative, Ashford*)

Dr Rupa Huq MP (*Labour, Ealing Central and Acton)*

Simon Jupp MP (*Conservative, East Devon*)

John Nicolson MP (*Scottish National Party, Ochil and South Perthshire*)

Jane Stevenson MP (*Conservative, Wolverhampton North East*)

Giles Watling MP (*Conservative, Clacton*)

The following Member was also a Member of the Committee during this Parliament: Julian Knight MP (Independent, Solihull)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at https://committees.parliament.uk/committee/378/culture-media-and-sport-committee/ and in print by Order of the House.

Committee staff

The current staff of the Committee are Rosie Akeroyd (Committee Specialist), Lucy Bishop (Committee Operations Assistant), Andy Boyd (Committee Operations Manager), Dr Conor Durham (Committee Specialist), Ollie Florence (Senior Media and Communications Officer), Seb Newman (Second Clerk), Olivia Rose (Media & Communications Officer), Joe Ryan (Committee Specialist), and Ben Sneddon (Clerk of the Committee).

Contacts

All correspondence should be addressed to the Clerk of the Culture, Media and Sport Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6188; the Committee's email address is CommonsCMS@parliament.uk.

You can follow the Committee on Twitter using @CommonsCMS

Contents

Summary

Connected technology is everywhere and influences every part of our lives. The Department for Culture, Media and Sport states that there is on average nine connected devices in every UK household, with a variety of uses. It is estimated that by 2050, there will be twenty-four billion interconnected devices worldwide. Networks of connected devices can create "smart environments", where networked devices work in concert to handle everyday tasks, across different spheres of life, such as in the home, urban environments, and workplaces.

Our inquiry focused on devices that displayed two fundamental characteristics: wireless connectivity to other devices and systems via the internet, and remote and/or autonomous operation. Connected tech can have a range of benefits, including improved efficiency, safety, security and health, environmental benefits and for entertainment. However, there are also a range of risks and harms associated with their use, including a loss of privacy, operational unpredictability and unfairness, online safety concerns and broadening patterns of domestic abuse.

We discuss data processing and privacy concerns in the home, in schools, in cities and at work. We recommend that the Government and Information Commissioner's Office address these issues by empowering users, and in particular children, to exercise their rights over their personal data through intuitive product design, clear terms and conditions and digital literacy schemes. We also evaluate some wider impacts of the Government's intentions to reform data protection legislation on international data flows and reform the regulator itself, and call on the Government to maintain data adequacy with the European Union and uphold the independence of the regulator.

We also explore safety and cybersecurity concerns for consumers and businesses when using connected technology. Our Report proposes ways to strengthen the new product security regime, which was based on the 2018 Code of Practice on Consumer Internet of Things Security, and ensure that the national regulator, the Office for Product Safety and Standards, is working effectively. We call on Government to address outstanding gaps in the regime created by a lack of action on improving security standards in workplace connected tech, device networks and data and cloud infrastructure. However, these interventions will be undermined if action is not taken to address the significant and persistent workforce gap in cybersecurity professionals and the shortage of core professional skills among cybersecurity professionals.

Our inquiry also explored the role of connected devices in broadening and exacerbating patterns of domestic abuse. We have found that tech abuse is becoming increasingly common. While there is no "silver bullet" for dealing with tech abuse, the Government can take more steps to tackle it by improving the criminal justice response, raising public awareness and convening industry to ensure manufacturers and distributors are mitigating risks through product design.

Introduction

1. Technology has come to influence every part of our lives. A smart speaker may wake you with an alarm and play the radio. Smart lights turn on automatically, set to a schedule. A wearable fitness tracker monitors your sleep and activity levels. Your smart doorbell rings and, through your smartphone interface, you see it is a parcel that you have been tracking. As you travel, connected cars with on-board virtual assistants and satellite navigation provide traffic updates, diagnostics infotainment and vehicle-to-vehicle and vehicle-to-infrastructure communication, while smartphone apps help people navigate public transport or utilise bike-, scooter- and car-sharing services. At work, your job may integrate all sorts of smart tech, from mundane devices like printers in a smart office to seemingly futuristic kit such as autonomous robots in a smart factory. At home, you might use a smart TV to stream or cast programmes that have been recommended to you based on previous viewing habits, while a smart home hub controls your heating. Further advances in technologies like autonomous vehicles, artificial intelligence and augmented and virtual reality may be on the cusp of integrating into our lives in new ways. Whether this picture presents something utopian or dystopian, it is clear that smart and connected devices are becoming more ubiquitous and increasingly sophisticated, even where they have augmented seemingly quotidian aspects of life.

The spread of connected tech

2. It is estimated that by 2050, there will be 24 billion interconnected devices worldwide.[1] In the UK alone, there will likely be 61 million smartphone users by 2024.[2] Evidence from the Department for Culture, Media and Sport (DCMS, previously the Department for Digital, Culture, Media and Sport) states that there is on average nine connected devices in every UK household, with a variety of uses.[3] A survey into connected homes found that 77 percent of UK adults own at least one smart home device, such as a smart speaker.[4] Health tech and security devices are particularly popular: techUK has found that 25 percent of the population own smart wristbands and smartwatches with built-in health monitoring technology and 29 percent of adults own a smart security and control device such as a smart doorbell, which incorporates motion detection, video feeds and smartphone notifications.[5]

3. However, the application of connected devices also extends well beyond our homes, into almost every sphere of life. Connected cars, for example, are increasingly coming to market with functionality ranging from enhanced safety, security and emergency assistance features to on-board voice assistants and entertainment systems to vehicle-to-vehicle connectivity and remote operation.[6] The market for connected technology in industrial and manufacturing domains is expected to grow to $200 billion by 2030.[7] There are also initiatives in the UK and globally to create "smart cities", where connected tech is deployed in the delivery of public services and functioning of local government.[8]

1 Big Brother Watch (TEC0052)
2 Department for Digital, Culture, Media and Sport (TEC0054) para 5
3 Department for Digital, Culture, Media and Sport (TEC0054)
4 techUK (TEC0049)
5 techUK (TEC0049)
6 Qq54–62
7 Department for Digital, Culture, Media and Sport (TEC0054) para 4
8 Information Commissioners Office (TEC0051) paras 38–40

What is "connected technology"?

Definition

4. Broadly speaking, "connected technology" refers to any (type of) physical object that is connected to the internet or other digital networks. Our inquiry focused on devices that displayed two fundamental characteristics:

- **Wireless connectivity** to other devices and systems via the internet (e.g., to share information or enable functionality through cloud computing)
- **Remote and/or autonomous operation** (e.g., to facilitate self-governing functionality, decision-making, interactivity, personalisation and so on).

The network (or networks) of connected devices is often described as "the Internet of Things" (IoT), which emphasises the increasingly connected nature of physical objects.[9] Connected devices may also be referred to as IoT or IoT-enabled devices, connectable devices, smart devices (where they operate autonomously), wearables or body-borne devices (where they are carried or worn on the body) and so on.

Components

5. As the UK's data protection authority, the Information Commissioner's Office (ICO), notes, connected technology is a "nexus" of many different technologies.[10] This may include sensors (components that detect events or changes in its surrounding environment), processors (that respond to and execute instructions), actuators (that control or move a device), software (the programs, instructions and data that run the device) and firmware (low-level programs that boot up and operate the device's hardware), cloud computing (dispersed computing services, such as data storage or processing, available over the internet and typically on-demand),[11] connectivity protocols and standards (rules that dictate how data is sent between and across devices, networks, servers, etc), artificial intelligence (AI), data analytics, machine learning and other technologies.[12] The confluence of technologies involved can make connected tech difficult to understand. Indeed, connected devices are often treated as a "black box", where the inner workings are obscured and consideration is only given to inputs and outputs.

6. One way to demystify the workings of connected devices is to consider the component technologies. One way to do this is to look at the "stack", where components are divided into layers that run on top of one another to form a complete system (see Figure 1). For connected devices, this might include:

- The device itself, which may be further delineated between:
  - the device's hardware (such as sensors, actuators, batteries, etc)

9 *Regulating the Internet of Things*, Debate Pack 2019/0221, House of Commons Library, 2 October 2019

10 Information Commissioners Office (TEC0051) para 11

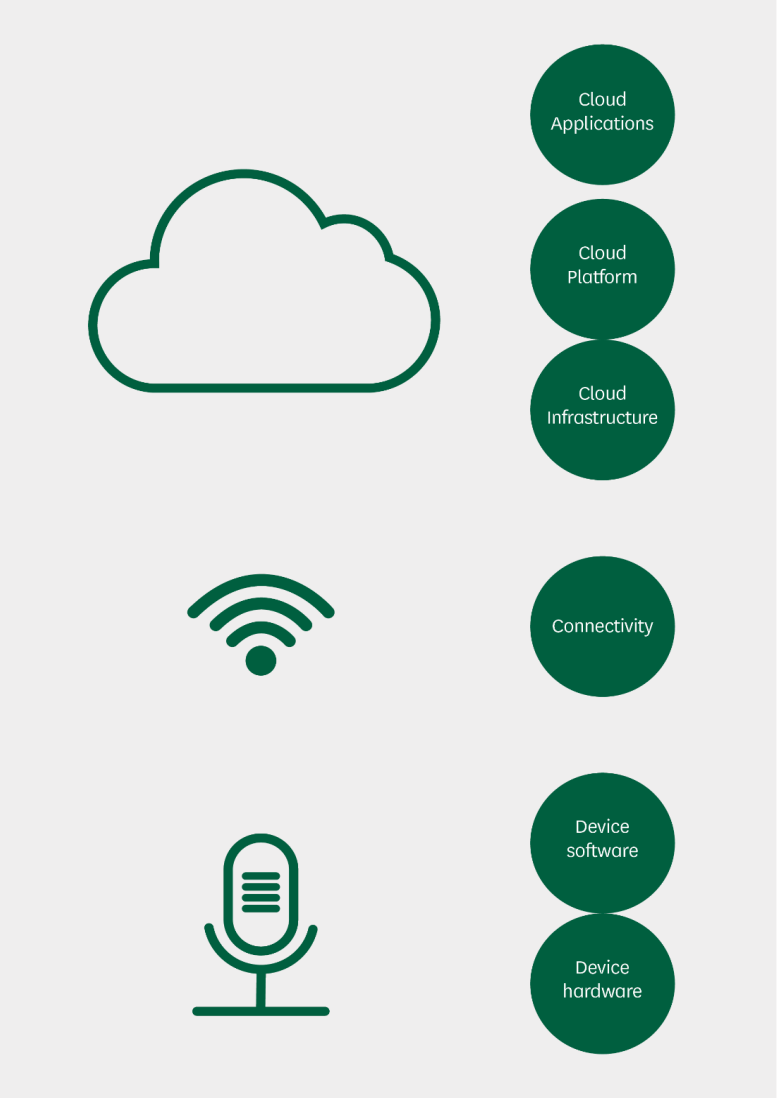
11 *Cloud computing*, POSTnote 629, Parliamentary Office of Science and Tech, June 2020

12 Dr Efpraxia Zamani (TEC0011); Dr Subhajit Basu (TEC0037); REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); Horizon Digital Economy Institute, University of Nottingham (TEC0046); 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 (TEC0048); Information Commissioners Office (TEC0051) para 11; Big Brother Watch (TEC0052) para 2; Department for Digital, Culture, Media and Sport (TEC0054)

- the device's software, which controls the device's functionality;

- Connectivity, which enables the device to exchange information with other devices or systems, using protocols such as Bluetooth, Ethernet, Wi-Fi and cellular networks like 4G and 5G;
- Cloud computing infrastructure, which provides the necessary hardware, storage and network for the overarching cloud system, and cloud platforms, which centrally manage, process and analyse data collected by connected devices and monitor and manage the devices themselves; and
- Applications, which run on top of the cloud platform and allow the end user to interface with the system.

Figure 1: Connected Tech



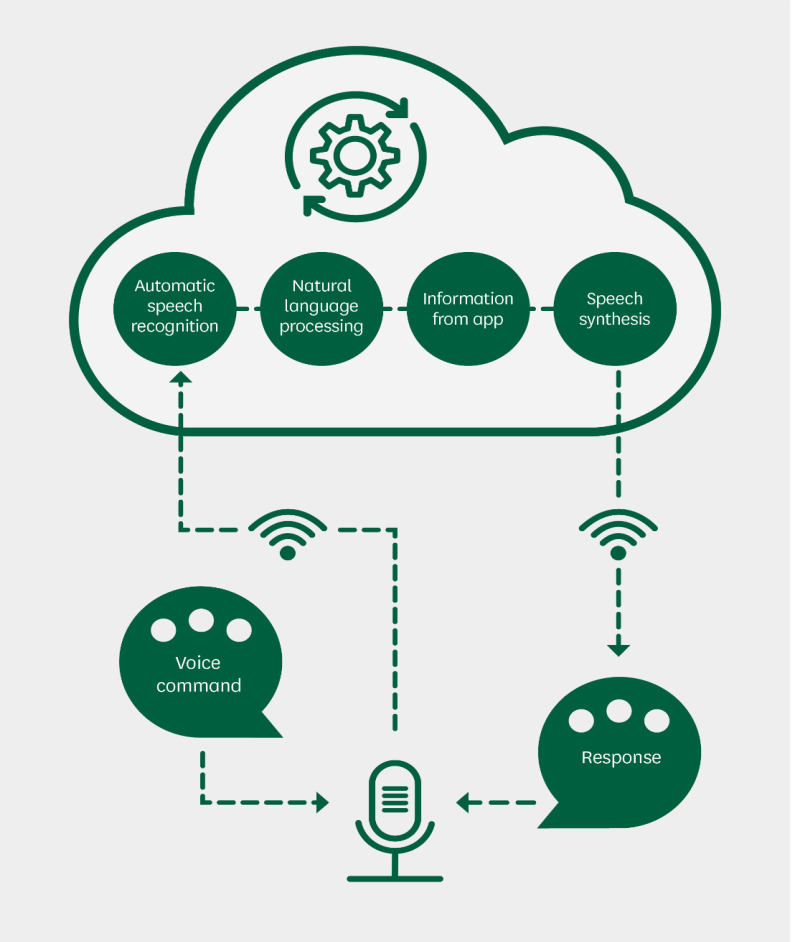
A simplified, illustrative example is provided in Box 1.

Box 1: Illustrative example of a voice activated smart speaker

Consider the example of a voice-activated smart speaker responding to an enquiry about the weather with reference to the system's components. First, the smart speaker's built-in microphones (hardware) register the sound of the voice command. The smart speaker's software will perform some simple processing to match the acoustic properties of the command to the phonetics of commands it is programmed to respond to and, if accepted, will activate the device. Next, a recording of the command will be sent via the speaker's Wi-Fi connection to the cloud platform for storage and more complex processing. The command will then be converted to text and parsed (through Automatic Speech Recognition and Natural Language Processing methods) so the system can understand the intent of the command. The system will then retrieve the requested information from an app (in this instance, from a weather service). The information will then be converted to speech in the cloud (through Speech Synthesis methods, which artificially produce human voices), sent back to the device and then communicated to the user via an in-built speaker.

A diagram is provided in Figure 2.

Figure 2: Connected Tech



7. In smart urban or enterprise environments, additional layers may be added to manage the large amounts of data that are collected and analysed. Where the system incorporates many devices, the stack might incorporate a gateway, for example, which acts as a router or server that connects a multitude of other devices to the internet and aggregates, processes and analyses data and transmits commands to and from those devices at once. To cut down on latency, particularly where there are large quantities of data being transferred, the stack may also incorporate "edge computing", where data processing and analysis happens on data servers in close geographical proximity to devices in the network, alongside or instead of cloud services (which are dispersed and usually not geographically proximate).[13] One use for edge computing might be in delivering public services in urban environments by ensuring data does not need to travel back and forth to a remote cloud computing data centre, which cuts down latency and allows the device to work faster, mitigating the risk of service outages caused by delays in data transmission.[14]

Applications and potentials

8. At the most macro-level, networks of connected devices can create "smart environments", where networked devices work in concert to handle everyday tasks, across different spheres of life.[15] Voice assistants, wearable devices, smartphones and smart speakers, appliances, doorbells and thermostats may collectively create "smart homes". Gigabit capable connectivity and big data analytics underpin greater automation, analytics and resource allocation in education, healthcare, utilities, waste management, policing and public and private transport in "smart cities", which are being developed by initiatives in the UK and across the world. Industrial robotics and AI are being deployed in "smart workplaces" ranging from offices and vehicles to smart factories and warehouses (with this rapid industrial and societal shift often referred to as the Fourth Industrial Revolution or Industry 4.0). Looking to the future, DCMS said that the applications of connected tech will grow further "due to innovations in areas such as the metaverse, human augmentation and industrial control systems".[16]

Benefits and harms

Potential benefits of connected tech

9. Contributors to our inquiry discussed the broad range of benefits of connected devices. The cited benefits included:

- **Improved efficiency, productivity innovation and service provision** in the home, at work, in education, regarding public services (such as energy, water, transport, healthcare, social care, procurement) and so on;[17]

13 Dr Cigdem Sengul (TEC0016); Horizon Digital Economy Institute, University of Nottingham (TEC0046); Information Commissioners Office (TEC0051); see also *Edge computing*, POSTnote 631, Parliamentary Office of Science and Tech, September 2020

14 "*Smart Cities need edge computing*", TechRadar, 29 April 2022

15 Dr Efpraxia Zamani (TEC0011); Information Commissioners Office (TEC0051)

16 Department for Digital, Culture, Media and Sport (TEC0054) para 31

17 The University of Gloucestershire (TEC0020); Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); Horizon Digital Economy Institute, University of Nottingham (TEC0046); techUK (TEC0049); AMDEA (TEC0056); Information Commissioners Office (TEC0051); Department for Digital, Culture, Media and Sport (TEC0054)

- **Improved safety and security** through connected alarm systems, external and internal camera systems, baby monitors, smart locks and doorbells and smart detectors for smoke and gas;[18]
- **Enhancing quality of life** by enabling people to live at home for longer and more independently, expanding the capabilities and capacity of social care, at-home healthcare wider support networks (such as activity tracking and carer alert technology), and improving the accessibility and practical applications of technology (such as using voice assistants instead of screen-based technologies);[19]
- **Health benefits** ranging from app-based monitoring and wearable health monitors to smart and AI-embedded healthcare ecosystems and research applications;[20]
- Direct and indirect **environmental benefits** ranging from more energy-efficient technologies and energy and environmental monitoring to planning and operational approaches in the energy sector (such as forecasting and optimising demand and supply based on factors such as consumer demographics, weather and time-of-day);[21] and
- **New potentials for entertainment and stimulation**, whether this in in the home, through domestic devices such as smart televisions, smart speakers and augmented and/or virtual reality (AR and VR respectively) hardware, or expanding the possibilities of art, culture and the creative industries.[22]

Barriers to realising benefits

10. Many submissions argued that these benefits were often not accessible to all.[23] This refers to a series of related concepts, including "digital exclusion", "digital poverty" and/or "digital inequality". A report published in March 2022 by the UK's communications regulator Ofcom identifies three types of "digital exclusion" among UK adults: where people have no access to the internet at home or elsewhere; where they lack the skills and/or confidence to use digital services safely and knowledgeably; and/or where they struggle to afford access to the internet and so either experience financial strains to retain access or go without altogether.[24]

18 Horizon Digital Economy Institute, University of Nottingham (TEC0046); techUK (TEC0049)

19 Dr Efpraxia Zamani (TEC0011); The University of Gloucestershire (TEC0020); Horizon Digital Economy Institute, University of Nottingham (TEC0046); techUK (TEC0049);Electrical Safety First (TEC0055); UK Research and Innovation (UKRI) (TEC0062)

20 Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); techUK (TEC0049); AMDEA (TEC0056)

21 REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); 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 (TEC0048); techUK (TEC0049); AMDEA (TEC0056)

22 techUK (TEC0049); AMDEA (TEC0056); Dr Rama Kanungo (TEC0057)

23 Dr Efpraxia Zamani (TEC0011); Dr Cigdem Sengul (TEC0016); The Centre for Care, University of Sheffield (TEC0017); Dr Subhajit Basu (TEC0037); University of Exeter, Coastline Housing (TEC0040); Internet Matters (TEC0044); Big Brother Watch (TEC0052)

24 Ofcom, *Digital exclusion: A review of Ofcom's research on digital exclusion among adults in the UK* (30 March 2022); Dr Efpraxia Zamani (TEC0011); see also The British Academy, *Understanding digital poverty and inequality in the UK* (November 2022)

11. Digital exclusion affects millions of people across the UK. It is estimated that 6 percent of households do not have access to the internet at home[25] and 19 percent of adults do not have fundamental digital skills.[26] Digital exclusion also typically intersects with other types of inequalities.[27] For example, the proportion of people without access to internet increases to 26 percent of people aged 75+ and 30 percent of people aged 65+ in deprived socioeconomic households.[28] Communities in poorer, rural areas typically experience poor internet connectivity;[29] these areas are often described as "not-spots" or "partial not-spots".

12. We have made recommendations to Government on tackling digital exclusion in several previous Reports, including on the *Impact of Covid-19 on DCMS sectors*[30] and *Broadband and the road to 5G*.[31]

Potential harms of connected tech

13. Many submissions discussed a broad range of risks and harms from the prevalence of connected tech:

- The **loss of privacy, lack of consent and erosion of other civil liberties** due to the volume and granularity of data collection, pervasiveness of monitoring and surveillance and "datafication" of daily life;[32]
- The **unpredictability and unfairness** of autonomous systems, mystifying decision-making and creating barriers to recourse;[33]
- Concerns about the **security and safety of devices**, ranging from giving malicious actors the ability to cause physical, financial and other types of damage or otherwise becoming safety hazards in their usage;[34]
- **Online safety-related concerns**, with physical devices and metaverse applications surfacing harmful content, particularly to child users;[35]

25 Internet Matters (TEC0044)
26 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 (TEC0048)
27 Big Brother Watch (TEC0052)
28 Dr Cigdem Sengul (TEC0016) para 2.1
29 techUK (TEC0049)
30 Digital, Culture, Media and Sport Committee, Third Report of Session 2019–21, *Impact of COVID-19 on DCMS sectors: First Report*, HC 291, paras 100–109
31 Digital, Culture, Media and Sport Committee, Fourth Report of Session 2019–21, *Broadband and the road to 5G*, HC 153, paras 70–71
32 Dr Cigdem Sengul (TEC0016); Dr Ana Canhoto; Professor Ashley Braganza; Dr Asieh Tabaghdehi (TEC0018); Sarah Turner; Dr Jason Nurse (TEC0029); Dr Subhajit Basu (TEC0037); Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); Internet Matters (TEC0044); Horizon Digital Economy Institute, University of Nottingham (TEC0046); 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 (TEC0048); Information Commissioners Office (TEC0051); Big Brother Watch (TEC0052); Radiocentre (TEC0058); Age Check Certification Services Limited (TEC0059); (ISC)2 (TEC0066)
33 Dr Subhajit Basu (TEC0037); Information Commissioners Office (TEC0051)
34 Dr Efpraxia Zamani (TEC0011); Dr Cigdem Sengul (TEC0016); Sarah Turner; Dr Jason Nurse (TEC0029); Information Commissioners Office (TEC0051); Big Brother Watch (TEC0052); Electrical Safety First (TEC0055); AMDEA (TEC0056); UK Research and Innovation (UKRI) (TEC0062)
35 Internet Matters (TEC0044); The University of Manchester (TEC0064)

- Concerns about how **sexual and/or domestic abuse** (referred to as "tech abuse") have become enabled by connected devices;[36]
- The potential **negative impact on radio** by the prevalence of smart speakers, streaming services and other integrated online platforms, due to reduced findability/discoverability of radio stations, crowding out of public service and public interest broadcasting, siphoning revenue from overlaid advertising, and manufacturers' gatekeeping, self-promotion and prioritising favoured third parties;[37]
- The broad **environmental impacts** throughout the lifecycle of connected devices, from the precious metals and minerals (including the "conflict minerals" tin, tungsten, tantalum and gold) and carbon emissions at the manufacturing stage (where the vast majority of emissions occur), to the energy use from individual products, digital infrastructure and data centres, to the toxic waste generated from improper or premature disposal of devices;[38]
- **Inefficiency delivering public services** when electronic systems are disrupted or fail entirely with no redundant systems in place;[39]
- The **health and social impacts**, such as children spending more time engaging with connected devices like AR/VR headsets and less time physically active or connected tech disrupting workers' employment rights and work-life balance.[40]

Our inquiry

14. We launched our inquiry in May 2022 to consider the applications of connected devices in various contexts and the potential benefits and harms that might manifest as a result. We received over sixty written submissions and held six evidence sessions with stakeholders and representatives from academia, civil society, the tech sector, the creative industries, the ICO and Government. This inquiry follows the work we undertook since 2020 through our Sub-Committee on Online Harms and Disinformation on *Online harms and the ethics of data*,[41] hearing from academics and experts, journalists, representatives from TikTok and the previous Information Commissioner Elizabeth Denham CBE. We also visited the Republic of Korea (as well as for our *Promoting Britain abroad*[42] and online safety[43] inquiries), where we met with parliamentarians, officials, content creators, device manufacturers and digital infrastructure providers, and the ABBA Arena in Newham, where we met with producers exploring the entertainment potentials of emerging technology.

36 Refuge (TEC0012); Dr Leonie Tanczer (TEC0021)
37 Radiocentre (TEC0058); News UK (TEC0063)
38 John Dodson (TEC0022); Tanja Katarina Rebel (TEC0023); 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 (TEC0048); The Restart Project (TEC0053)
39 Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
40 Internet Matters (TEC0044)
41 Culture, Media and Sport Sub-Committee on Online Harms and Disinformation, 'Online harms and the ethics of data,' accessed 31 May 2023
42 Digital, Culture, Media and Sport Committee, Second Report of Session 2022–23, *Promoting Britain abroad*, HC 156
43 Culture, Media and Sport Sub-Committee on Online Harms and Disinformation, 'Online safety and online harms,' accessed 31 May 2023

15. We are grateful to everyone who contributed to this inquiry. However, while we heard from many interesting and insightful voices, we were disappointed that, despite being a market leader in smartphones, tablets and wearables and a notable manufacturer of smart speakers, Apple did not constructively engage with our inquiry or accept our invitation to give oral evidence, in contrast to its more proactive competitors Amazon and Google. Apple should seek to rectify this by engaging with the issues raised in this report.

16. After our inquiry concluded taking oral evidence, the Government announced that it would be making changes to the remits of several departments, including DCMS, whose work we scrutinise. This resulted in the creation of a dedicated Department for Science, Innovation and Technology (DSIT), to be led by the now former-Culture Secretary Michelle Donelan and with Minister Julia Lopez taking up ministerial roles in both departments. In response to these machinery of government changes, this will be our last substantive inquiry that predominantly falls within the digital policy portfolio, though we retain an interest in matters where digital and technology policy intersect with the culture, media and sport sectors, including music streaming, video-on-demand, gambling, mis- and disinformation and the use of AI in the creative industries.

Our report

17. We have responded to the change in our remit amid our inquiry by delineating our work into two reports. Taken together, these cover the range of issues we uncovered throughout this inquiry and our aforementioned *ethics of data* work, concluding our work within the digital portfolio while reaffirming our scrutiny of the application of technology in the culture, media and sport sectors.

18. This report considers three key aspects, covering some of the aforementioned risks and threats that need to be mitigated in order to fully realise the benefits of connected tech:

- Chapter 1 discusses data and privacy concerns in the home, in schools, in cities and at work. It also considers some wider impacts of the Government's intentions to reform data protection legislation on international data flows and reform the regulator itself.
- Chapter 2 explores safety and cybersecurity concerns for consumers and businesses, and how the cyber workforce shortages are undermining the response to these concerns.
- Chapter 3 examines the role of connected devices in broadening and exacerbating patterns of domestic abuse.

19. Our second report, to be published later in the summer, will conclude our inquiry by considering the impact of connected technology and AI in and on the creative industries, with a particular focus on the impacts on copyright, skills and online safety.

1 Data and privacy

20. Connected devices, by virtue of their component technologies like sensors, trackers, voice assistants and automation such as algorithms, machine learning and AI, typically process large quantities of data that may assist or underpin device functionality. "Processing" refers to a range of activities, including collecting, recording, using, analysing, combining, disclosing or deleting data.[44] As the ICO observes, in the context of connected tech, this data is "often highly personal […] about people who use it and people who are exposed to it", ranging from biometric data used in voice or facial recognition to geolocation data captured by wearables and smartphones.[45] The activities involved in data processing are regulated by the UK's data protection framework, which aims to ensure that people "can have trust and confidence in how their data is used and that risks of harm are mitigated".[46]

21. The current UK data protection framework is set out in the Data Protection Act 2018, which includes data protection regimes on general processing, law enforcement processing and intelligence services processing.[47] It sits alongside and is supplemented by the UK General Data Protection Regulation (GDPR), which sets out key areas including the specific regulatory principles, the rights of individuals over their personal data, obligations on data controllers (people who decide how and why to collect data) and processors (people who do the processing), enforcement mechanisms and associated remedies, liabilities and penalties.[48] Under data protection law, the term "personal data" refers to data that relates to an identified or identifiable individual (known as a data subject).[49] The term "special category data" refers to types of personal data that are particularly sensitive, and applies to racial or ethnic origin, political opinions, religious or philosophical believes, trade union membership, genetic and biometric data, and data concerning a person's health, sex life and sexual orientation.[50]

22. In order to process personal data, a data controller (a person or organisation that exercises overall control over the purposes and means of the processing) must have an appropriate, valid lawful basis, of which six are set out in UK GDPR: the individual has given consent; it is necessary to fulfil a contract; it is necessary to comply with legal obligations; to protect someone's life (i.e., vital interests); or to perform a public task; or it is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.[51] Legitimate interests is the most flexible lawful basis for processing, but necessitates taking on extra responsibility for considering and protecting people's rights and interests; the ICO's guidance states that "it helps to think of this as a three-part test", where a processor must identify a legitimate interest, show that the data processing is necessary to achieve it, and balance it against an individual's interests, rights and freedoms.[52]

44 Information Commissioner's Office, Introduction to data protection: some basic concepts,' accessed 20 April 2023
45 Information Commissioners Office (TEC0051) para 5
46 Ibid., para 10
47 Information Commissioner's Office, 'About the DPA 2018,' accessed 20 April 2023
48 Regulation (EU) 2016/679
49 Information Commissioner's Office, 'What is personal data?,' accessed 20 April 2023
50 Information Commissioner's Office, 'Special category data,' accessed 20 April 2023
51 Information Commissioner's Office, 'A guide to lawful basis,' accessed 2 June 2023
52 Information Commissioner's Office, 'Legitimate interests,' accessed 2 June 2023

Connected tech in the home

Privacy and surveillance

23. The majority of submissions to our inquiry cited the risks of excessive surveillance and datafication and the impact on privacy as the primary challenges posed by connected technology.[53] Data collection and processing is fundamental to the utility of connected tech, both for consumers, operators and manufacturers. Directly, user data enables functionalities like monitoring, measuring and tracking (e.g. for fitness wearables), activation (e.g. for smart speakers), customisation, issuing alerts, notifications and recommendations, initiating interventions (e.g. in healthcare solutions) and decision-making, reasoning and other types of remote and/or autonomous operation.[54] Indirectly, data can also be leveraged and repurposed for other means, such as product development, targeted advertising (based on observed or inferred preferences) and data sharing with third parties like business partners and advertisers.[55]

24. Contributions from industry have noted that data processing is not *prima facie* itself harmful. As Antony Walker, Deputy CEO of tech UK, the British trade association for the tech sector, argued, "we should not simply use the terms 'data collection' and 'data aggregation' and assume that all of that is for a purpose that has negative connotations or could bring risk" but instead "focus in on the risk and take a risk-based approach to thinking about the implications of this data being gathered and the extent to which it is appropriate for it to be stored, and about the purposes that it may then be used for, which we might say it should not be used for".[56]

25. Information Commissioner John Edwards similarly asserted that "recognising that to deliver what [manufacturers and distributors] promise requires a transmission and a use of data does not necessarily mean that there is an intrusion on our privacy, as long as that occurs within the expected foreseeable bounds".[57] Regarding connected devices in the home specifically, the Commissioner asserted that his "confidence in the products that I have chosen that they are not listening to comments that I make without the command preceding them, and that they are not recording, processing and using information from my flat in ways that are inconsistent with the undertakings that are on the privacy policy or written on the box".[58] He extrapolated that this perspective was relatively widespread, insisting that concerns about data did not feature in complaints statistics and that "the confidence that the market expresses in these devices partly reflects the expectation and belief that an office such as mine exists and is there to ensure that those devices are not used in unexpected ways, or that the data has not been used in ways that would be inconsistent with the foreseeable consumer expectation of the data flows and the use of the device".[59]

53 Qq2, 12–14, 18, 35; Dr Cigdem Sengul (TEC0016); Dr Ana Canhoto; Professor Ashley Braganza; Dr Asieh Tabaghdehi (TEC0018); Sarah Turner; Dr Jason Nurse (TEC0029); Dr Subhajit Basu (TEC0037); Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); Internet Matters (TEC0044); Horizon Digital Economy Institute, University of Nottingham (TEC0046); 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 (TEC0048); Information Commissioners Office (TEC0051); Big Brother Watch (TEC0052); Radiocentre (TEC0058); Age Check Certification Services Limited (TEC0059)

54 Dr Efpraxia Zamani (TEC0011) para 4.3

55 Ibid.

56 Q51

57 Q283

58 Qq312–4

59 Qq283, 314

26. Despite this, our inquiry has exposed several issues in taking the proliferation of devices as indicative of widespread consumer confidence at face value. Indeed, the Commissioner did recognise some limitations to his own statistics, noting that "we do not have good data to know if that absence [of complaints in the ICO's statistics] is a result of ignorance of some harms that are being caused, or an acceptance that there is a transaction that is involved in purchasing and installing one of these devices".[60] However, more fundamentally, many people may continue to use digital services or purchase devices even though they are aware that manufacturers or developers use their data in ways that infringe on their privacy, target them with advertising and so on; this contradiction is often referred to as the "privacy paradox".[61] Dr Jeni Tennison, Vice-President of the Open Data Institute (ODI), and Dr Jiahong Chen, Research Fellow in IT Law at the Horizon Digital Economy Institute, University of Nottingham, further explained during our *Online harms and the ethics of data* inquiry that this paradox can be explained by a sense of "digital resignation", where people understand and feel resigned to data processing practices as the price for participating in the digital economy, rather than because of a misunderstanding or misestimation of benefits and risks to the processing of personal data.[62] In many, if not most, instances, terms and conditions are often vague, complex, lengthy and enabling, contributing to this sentiment.[63] Dr Efpraxia Zamani, Senior Lecturer in Information Systems at the University of Sheffield Information School, similarly submitted that "terms and conditions and informed consent texts are so complicated that prior research has suggested that consumers do not consent to data sharing but rather 'surrender' their data".[64] Dr Zamani added that this problem is particularly acute for otherwise-excluded social groups, who "feel obliged in some way to part with their data, because they feel that not doing so can have further negative implications for them".[65]

27. Academic evidence instead argued that enabling consumers was the best way to address digital resignation. Dr Cigdem Sengul, Senior Lecturer in Computer Science at Brunel University London, submitted that:

> the 1973 US Department of Health, Education and Welfare report on 'Records, Computers, and Rights of Citizens' still effectively captures the current situation on the right of citizens in the presence of technological advancements: 'the net effect of computerisation is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems [and] although there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms.[66]

A submission from the Oxford Internet Institute (OII) similarly advocated that:

> in the long term, regulating big tech companies to mandate practices that return as much control over personal data back to individuals, enabling

60 Q283
61 Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
62 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 13 October 2020, HC (2020–21) 646, Qq193–5; see also Ana Canhoto, 'The cultivation of digital resignation', 23 April 2021
63 Big Brother Watch (TEC0052) para 14
64 Dr Efpraxia Zamani (TEC0011)
65 Ibid.
66 Dr Cigdem Sengul (TEC0016) para 3.1

> some level of personal control and educating consumers to make active choices when using smart connected technologies may help to address the root cause of digital resignation.[67]

28. Beyond personal privacy, the use of connected tech in homes can also impact others.[68] As Big Brother Watch illustratively describes:

> Smart doorbells, with live video cameras, audio capture and sometimes even facial recognition capabilities, are one of the most popular home smart devices. Smart doorbells collect data not only on the individual users, but visitors to their properties and often, other people within view on the street or immediate area beyond their property bounds. Amazon's Ring doorbell [a smart home product produced by its subsidiary home security device manufacturer Ring, acquired in 2018] can capture audio from up to twenty metres away. This has led to legal disputes and some individuals will understandably be concerned about their neighbours' uses of surveillance devices.[69]

News reports have revealed that alongside the data captured, Amazon keeps records of every motion detected by its Ring devices and has provided its research and development team with access to every Ring video that has been created.[70] Users installing such devices may be unaware that in doing so they become data controllers with legal obligations under the Data Protection Act.[71] Leila Rouhi, Vice-President of Trust and Privacy for Amazon Alexa, responded to these concerns, asserting that the company provides features like indicator lights and stickers on cameras to notify when recording is happening, motion detection zones and privacy zones that control what triggers a recording or blacks out areas, and provide guidance on how to install the device.[72] However, it is the user who sets these terms, rather than those who might also reasonably be captured by such technology, like neighbours, visitors and others.

Exercising data rights

29. As noted, the rights of data subjects over their personal information are a key part of the data protection framework, and indeed to enabling data subjects to exercise control over how their data is processed. There are eight data subject rights provided by the GDPR, including rights to be informed about data collection and use, to access their personal data, to rectify inaccurate and incomplete personal information, of erasure and to restrict and/or to object to data processing, as well as when personal data is used in automated decision-making and/or profiling.[73] Some of these rights are also impacted by the lawful basis on which the data subject's personal data is processed: where the lawful basis is consent, for example, a data subject does not have the right to object, but does have the right to withdraw consent (which either way should prevent further processing).[74]

67 Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
68 Dr Efpraxia Zamani (TEC0011); Dr Cigdem Sengul (TEC0016); Sarah Turner; Dr Jason Nurse (TEC0029); Big Brother Watch (TEC0052)
69 Big Brother Watch (TEC0052) para 9
70 Ibid., paras 15–6
71 Ibid., para 9
72 Qq334, 353
73 GOV.UK, 'Data protection,' accessed 2 June 2023
74 Information Commissioner's Office, 'A guide to lawful basis,' accessed 2 June 2023

30. However, there are several features inherent to connected tech that may make it difficult for people to exercise their data rights. First, connected devices are often designed without an obvious or intuitive user interface, like a computer screen. As the Information Commissioner explained, "some of these are just sensors that are collecting and transmitting data about the user with no real ability for the user to meaningfully interact with it", which "does present a number of challenges".[75] The lack of or relatively simple interfaces, for example, can mean that the device's data processing and connectivity are less visible or indeed hidden to the user, as complex information cannot be conveyed comprehensibly by the device and interacted with in simple and obvious ways.[76] Often, users can only interface with devices through smartphone apps, which they may not necessarily be aware of, know how to use or even have access to, particularly in the case of children, older people and/or the digitally-excluded.[77]

31. Second, people may not have the levels of digital literacy to operate devices in a privacy-protecting way. David Kleidermacher, Vice-President of Engineering for Android and Made-by-Google Security and Privacy at Google, and Amazon's Leila Rouhi noted several times that their products provide apps, notifications and settings functions to allow users to opt into or access greater privacy controls.[78] However, as Dr Lulu Shi, departmental lecturer at the University of Oxford and postdoctoral researcher at the OII told us, this requires active intervention by digitally-literate users rather than by default.[79] Without the requisite understanding, users may not therefore be able access these opt-ins/opt-outs and controls.

32. Finally, people may not know about their data rights, and may not understand how, or have the resources, to fully exercise their data rights when in contact with connected tech. As Carly Kind, Director of the Ada Lovelace Institute, explained "most people do not feel empowered to exercise their data rights, either because they don't know them or they don't know how to exercise them, or the barrier for exercising them is quite high because it requires either you go to the ICO or you get a lawyer".[80]

33. Recent reports have demonstrated these challenges. On 31 May 2023, since our inquiry concluded, it was reported that Amazon and its subsidiary Ring had agreed to pay $25 million and $5.8 million respectively to the US Federal Trade Commission (FTC) in settlements with the US Department of Justice (DOJ) for privacy violations pertaining to its connected products.[81] According to the FTC complaint, Amazon's Alexa voice assistant violated children's privacy rights, because it had retained children's voice recordings indefinitely, failed to honour deletion requests for users' voice recordings and geolocation data and failed to notify customers that it had not honoured their requests, in order to train their algorithms.[82] A statement from Amazon responded that "while we disagree with the FTC's claims and deny violating the law, this settlement puts the matter behind us, and we believe it's important to put the settlement in the right context", citing

75 Q279
76 Qq279, 296; Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
77 Sarah Turner; Dr Jason Nurse (TEC0029)
78 Qq340, 348–50
79 Qq12–13
80 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 13 October 2020, HC (2020–21) 646, Q186
81 "*Amazon's Ring used to spy on customers, FTC says in privacy settlement*", Reuters, 1 June 2023
82 "*FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests*", Federal Trade Commission press release, 31 May 2023

several privacy policies and protections.[83] The FTC complaint against Ring, meanwhile, alleged that the company had allowed "thousands of employees and contractors" to watch and download recordings of customers' private spaces for their own purposes, exposing customers to spying and harassment.[84] Reuters reported that Amazon similarly said that it disagreed with the allegations about Ring and that in February 2019 Ring changed its policies so that most employees or contractors could only access private recordings with that customer's consent;[85] in a statement to the BBC, Amazon said that "Ring promptly addressed the issues at hand on its own years ago, well before the FTC began its inquiry".[86]

34. Adding to the sense of resignation are reports that indicate that tech companies may rely on other lawful bases to process data beyond consent. While this *prima facie* does not preclude data processing for uses like targeted advertising, it does have implications for what data rights may be exercised and how users' rights and freedoms should be balanced (particularly where the lawful basis is more flexible, as with processing for "legitimate interests"). In July 2021, for example, it was reported that Amazon was fined €746 million (£636 million) by the Commission Nationale pour la Protection des Données (CNPD), Luxembourg's data protection authority,[87] on the basis that its advertising system was not based on "free consent", according to the original complaint made in 2018 by French civil liberties group La Quadrature du Net.[88] At the time of writing, Luxembourg's obligations of professional secrecy have prevented the CNPD from commenting on the case until the appeal process is concluded,[89] though Amazon has responded to the fine by saying "we believe the CNPD's decision to be without merit and intend to defend ourselves vigorously in this matter".[90] In January 2023, Meta Platforms, the parent company of Facebook and Instagram, was fined €390 million (£346 million) by Ireland's Data Protection Commission for requiring users to consent to changes to its terms of service before using its platforms, which allowed the company to process data in order to deliver targeted advertising, on the grounds that said data processing relied on the "contract" lawful basis, rather than "consent".[91] Meta has said that it intends to appeal the ruling.[92]

35. **Data rights are an important tool for empowering data subjects and balancing data processing against users' rights and freedoms. However, there are many barriers to individuals being able to exercise these rights when using or interacting with connected tech, ranging from product design to digital literacy and resources. Users must be given clear information about, and a fair chance to understand, the basis on which their data is used, the implications for their digital rights, the benefits and risks, and how to consent, object and how to exercise these rights.**

36. ***The Government should introduce appropriate measures to standardise privacy interfaces for connected devices as a first step, which will help users learn how to control connected devices in their homes and exercise data rights. Privacy interfaces should***

83 Amazon, 'Amazon's response to our recent settlement with the U.S. Department of Justice regarding Alexa,' 31 May 2023
84 "*Amazon to pay $25m over child privacy violations*", BBC News, 1 June 2023
85 "*Amazon's Ring used to spy on customers, FTC says in privacy settlement*", Reuters, 1 June 2023
86 "*Amazon to pay $25m over child privacy violations*", BBC News, 1 June 2023
87 "*Amazon hit with $886m fine for alleged data law breach*", BBC News, 30 July 2021
88 "*Why Amazon's £636m GDPR fine really matters*", Wired, 4 August 2021
89 "*Decision regarding Amazon Europe Core SARL*", National Commission for Data Protection press release, 6 August 2021
90 "*Amazon hit with $886m fine for alleged data law breach*", BBC News, 30 July 2021
91 "*Meta fined almost €400mn over EU privacy rule violations*", Financial Times, 4 January 2023
92 "*Meta fined €390m over use of data for targeted ads*", BBC News, 4 January 2023

be appropriately accessible, intuitive and flexible enough so users of a reasonable level of digital literacy and privacy expectations can use them, without requiring them to go through complex dashboards with long lists of terms and conditions and settings. Interfaces should also provide information on how devices are connecting to other devices and networks, to provide transparency about data flows.

Impacts on children

Connected toys and data collection

37. Concerns about surveillance and data processing equally apply to children. Sarah Turner, a doctoral researcher at the University of Kent, and Dr Jason Nurse, Senior Lecturer in Cyber Security at the University of Kent and Public Engagement Lead at Kent Interdisciplinary Research Centre in Cyber Security, have argued that children are "necessarily put in a position of vulnerability" due to the lack of ownership, control and education about connected devices in their home, and that devices themselves rarely prompted owners to review security or privacy settings.[93] Regarding connected toys specifically, Dr Sengul argues that "recent research finds that only one of the six privacy policies reviewed has a reading age close to the target age of the product" and that "consequently, in a recent study with young learners, we saw that young people, like adults, do not read the Terms and Conditions".[94] When our concerns were put to Julia Lopez MP, Minister for Data and Digital Infrastructure at DSIT and Minister for Media, Tourism and Creative Industries at DCMS, she responded that "it is difficult to answer questions like this, because it depends on the device, the type of data being collected, where the data is being retained and how long it is being stored".[95]

38. Despite our concerns, the Information Commissioner has argued that the ICO has lacked the resources to proactively anticipate and engage with the market. Instead, the regulator is reliant on companies themselves choosing to engage:

> We do not really have access to the product's launch time horizon, so we do not know what is coming down the pipeline—what is going to be in Hamleys next Christmas—and whether we should be in there. We do not have capacity to get ahead of that, but we are available […] if those companies choose to engage us.[96]

Stephen Almond, the ICO's Director of Technology and Innovation, continued that "our priority is in scrutiny of things such as gaming, video and music streaming and social media".[97] He added that "connected toys are an area that we would like to be able to turn to in future", but did not expand further on the constraints or how this ambition could be realised.[98] However, when the question of the regulator's capacity were put to the Minister, she implied that the ICO was satisfied with the current approach, responding that "the Information Commissioner has not expressed any concerns to me about resourcing levels on this issue".[99]

93 Sarah Turner; Dr Jason Nurse (TEC0029)
94 Dr Cigdem Sengul (TEC0016) para 3.5
95 Qq389–390 [Julia Lopez]
96 Q297 [John Edwards]
97 Q297 [Stephen Almond]
98 Q297 [Stephen Almond]
99 Qq389–390 [Julia Lopez]

Smart speakers and online safety

39. Emerging technologies, including connected tech are also vectors for online harm, and therefore theoretically within the ambit of the online safety regime. The Antisemitism Policy Trust has consistently raised concerns that Amazon's Alexa virtual assistant and other smart assistants have given antisemitic answers "to questions about Jews, Muslims, Israel and the Holocaust", even despite an internal inquiry by the company launched in November 2020.[100] In December 2021, it was reported that Alexa had suggested a dangerous challenge to a 10-year-old girl that involved touching a penny to the exposed prongs of a phone charger in a wall socket that it had found on the internet, which the company subsequently fixed.[101] Internet Matters, a not-for-profit organisation launched by UK internet service providers offering child safety advice, has further argued that the metaverse posed particular, including more visceral, threats to online safety above more familiar online harms.[102]

40. However, the user empowerment duties in the regime, which aim to enable users to reduce the likelihood they will encounter harmful content like content promoting suicide, self-harm or eating disorders or content that is abusive or incites hatred, will only apply to the largest user-to-user services as currently drafted. The former Secretary of State for Digital, Culture, Media and Sport, Rt. Hon. Nadine Dorries MP,[103] and the current Parliamentary Under Secretary of State for Culture Media and Sport, Lord Parkinson of Whitley Bay,[104] have clarified that, while not explicitly mentioned, the metaverse will be within the scope of the online safety regime as a user-to-user service.[105] However, smart speakers and voice assistants instead integrate search services to fetch responses to commands, which are not covered by the user empowerment duties within the Bill.

41. ***The Government should clarify the obligations in the Online Safety Bill for voice assistants, connected devices (like smart speakers) and other emerging technologies that can surface harmful content, to ensure that those that integrate search services in particular fall in-scope of the duties. It should also set out in its response to this report how the online safety regime will categorise voice assistants and connected devices that integrate internet search so that they do not service harmful content like hate speech and other harms.***

Connected tech in schools

42. Alongside the home, children are increasingly likely to interact with connected tech in schools as education technology (also known as edtech) becomes more prevalent.[106] There are two broad types of education technology: school management products and learning and skills products.[107] School management products include products like virtual learning environments and blended learning platforms such as Google Classroom and Canvas, which enable file-sharing, communication and assignment-setting and grading between teachers and students. Learning and skills products include apps and platforms

100 Antisemitism Policy Trust (TEC0010)
101 "*Alexa tells 10-year-old girl to touch live plug with penny*", BBC News, 28 December 2021
102 Internet Matters (TEC0044)
103 HC Deb, 19 April 2022, col 96 [Commons Chamber]
104 HL Deb, 24 January 2022, col 15 [Lords Chamber]
105 Carnegie UK Trust, 'Regulating the future: the Online Safety Bill and the metaverse', 4 February 2022
106 Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
107 Q27

that may be more widely available, such as Duolingo for language-learning. The OII has noted that education technology has brought improvements in many areas: Dr Lulu Shi told us that the most obvious benefit of education technology had been to help enable schooling following school closures during the Covid-19 pandemic.[108]

Impact of education technology

43. Dr Shi noted three primary risks to children associated with the use of connected products and software in educational environments: the vulnerability of children as data subjects; the particular potential harms from data collection and tracking; and product design.

44. First, children are particularly vulnerable, both because they may not understand or be able to access or acquire necessary and relevant information and because they are likely to use connected tech in contexts where they do not have the agency to protect their privacy and exercise their rights. There are several aspects to this. Many submissions argued that children, like adults with lower levels of digital literacy, may not understand the terminologies and technical information presented in products' terms and conditions, guidance, settings and user interfaces.[109] As a submission from the Horizon Digital Economy Institute at the University of Nottingham argued:

> Privacy policies are hardly understandable by the general public and even more difficult for vulnerable people such as younger or older people or people with mental disabilities. Privacy policies for children are especially confusing, difficult to comprehend, often long and complex, and while often it states a requirement for guardians' consent, it is not always actually required or checked.[110]

Additionally, it may also be difficult for children of certain ages to estimate the risks of certain behaviours (such as opting-in or opting-out of using connected devices) and anticipating outcomes (such as how data is being used).[111] As the OII argues, "research into children's understanding of online privacy risks, for example, has shown that they have a better understanding of interpersonal risks (e.g. sharing too much or sensitive personal information with someone and then regretting it) than they do of other types of data risk such as data breaches or future reputational damage".[112]

45. Children are also vulnerable because of the contexts in which they may become data subjects. Where organisations acquire and/or implement technology on behalf of students, the latter lack practical ways to opt-out.[113] Big Brother Watch highlighted an illustrative example in European case law relating to the data subject rights of children where, in February 2020, the Administrative Court of Marseille held that the use of facial

108 Q6; see also Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); UK Research and Innovation (UKRI) (TEC0062)

109 Dr Cigdem Sengul (TEC0016); Sarah Turner; Dr Jason Nurse (TEC0029); Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); Internet Matters (TEC0044); Horizon Digital Economy Institute, University of Nottingham (TEC0046); Big Brother Watch (TEC0052); see also oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 13 October 2020, HC (2020–21) 646, Qq217–23

110 Horizon Digital Economy Institute, University of Nottingham (TEC0046) para 11

111 Qq6–7;

112 Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)

113 Ibid.

recognition at two high schools was unlawful "because: (a) it was not a proportionate interference with student's right to privacy; and (b) there was no lawful basis for the use of facial recognition, as even if fully-informed, freely-given consent is given by students, the inherent power asymmetry in the school environment means consent can never be given to use of facial recognition in schools under the GDPR".[114]

46. Second, connected tech in the classroom may lead to the collection of massive amounts of both children's personal data (age, ethnicity, gender, etc) and behavioural data (how children learn, perform in school, what they do). This data can have a range of applications. As techUK's Deputy CEO Antony Walker argued, on the one hand, this data may be used to develop products, understand learning outcomes and provide teachers with feedback on student progress.[115] However, this data could be aggregated over long periods of time to create longitudinal datasets that then form the basis of predictive models, such as for online advertising, insurance companies, future employers and law enforcement that can have lasting impacts throughout the student's life.[116] Many educational products are available for free precisely because of the financial incentives associated with processing and selling data.[117] These factors together can further create a technological "lock-in" effect, where consumers are incentivised to continue using a product or technological standard and/or disincentivised from switching to alternative products or standards.[118]

47. Third, technologies that are being procured are often not designed by people with pedagogical training or teaching experience;[119] instead, design decisions are taken by engineers.[120] However, evidence from the OII argued that it is instead "teachers who are blamed as holding outdated attitudes and being resistant to technological innovations".[121] In many cases, this has led to teachers and students being of "second priority".[122] Dr Shi has called for control of technologies to be distributed equally amongst all stakeholders involved in the design process, including students, parents, teachers and education experts.[123]

48. However, the ICO rejected these concerns, with the Commissioner saying that "we do not see any evidence of harm appearing through education technology".[124] Mr Edwards instead mused that "if schools avail themselves of Google Docs and Microsoft 365—any kind of tech tool that is available for use in the classroom can be characterised as edtech, and that does not mean that there are unique threats to children through the use of those tools, or the mass harvesting of identifiable information about those student learners or users".[125]

114 Big Brother Watch (TEC0052) para 54
115 Q51 ff.
116 Qq50–51; see also see also Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
117 Q30
118 Q50
119 Q6; see also Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
120 Q28; see also Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
121 Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039)
122 Ibid.
123 Qq28–29
124 Q298
125 Q299

The Age-Appropriate Design Code

49. Data protection law maintains that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data".[126] The Age-Appropriate Design Code (also known as the "Children's Code") sets out fifteen risk-based standards (including one dedicated to connected devices and toys) by which services that are likely to be accessed by children should comply,[127] including that "the best interests of the child should be a primary consideration" in design and development in accordance with Article 3 of the United Nations Convention on the Rights of the Child (UNCRC).[128] Some standards set out in the Code include privacy settings automatically being set to very high, non-essential location tracking being turned off, children no longer being "nudged" to lower privacy settings through notifications and the implementation of clearer and more accessible tools to help children exercise their data protection rights.[129] Crucially, the Code requires services to establish age with an appropriate level of certainty or apply its standards to all users.[130]

50. The Code has been in force since 2 September 2021.[131] However, the ICO's Stephen Almond told us that a new version of the code will have to be adapted and laid before Parliament in line with data protection reform, though both the ICO and the Minister reaffirmed their ambition to maintain the Code's protection of children within the new regime.[132]

51. **The use of connected tech in schools and by children in homes raises concerns, including the harvesting and third-party use of children's data and their lack of control over what technology is used and when. The Government and ICO were quick to dismiss our concerns about this issue.** ***We urge the ICO to take a more proactive approach in engaging with manufacturers of connected toys and education technology. It should ensure that all products include: terms and conditions that are age-appropriate; privacy settings that are intuitive for children and help them exercise data rights; and fully explain the benefits and risks of data processing. Industry should be supported in this through comprehensive guidance, independent research and user-testing.***

52. ***The Government should commit to ensuring that the Age-Appropriate Design Code is strengthened rather than undermined by data protection reform and to laying the revised code as soon as is practicable.***

Smart cities

53. Connected technology is also increasingly being deployed in public, urban spaces known as "smart cities" (see paragraphs 3 and 8). However, just as smart cities provide a broader scale of opportunities, there are also additional risks to confidence in privacy and

126 Established in UK GDPR Recital 38; see also Information Commissioners Office (TEC0051)
127 Information Commissioner's Office, 'Age-appropriate design code: About this code,' accessed 26 April 2023
128 Information Commissioner's Office, 'Age-appropriate design code: Best interests of the child,' accessed 26 April 2023; see also Information Commissioners Office (TEC0051)
129 Information Commissioner's Office, 'The Children's code: what is it?,' accessed 27 April 2023
130 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 26 January 2021, HC (2020–21) 646, Q272 [Damian Hinds]
131 Information Commissioner's Office, 'The Children's code: what is it?,' accessed 27 April 2023
132 Qq301, 391

data protection. First, smart cities can become extreme surveillance environments that encourage continuous and large-scale data processing, including significant processing of geolocation data (which indicates the geographical location of a subject). As the ICO notes, "this may also lead to the processing of special category data (such as the potential to infer someone's religion or trade union membership by tracking the locations they visit)".[133] Additionally, the scale of data collection can present a lucrative target for cyberattacks.

54. Second, smart cities can obscure data processing to an even greater extent than in homes and schools, with little accountability as to how that data is used and/or repurposed.[134] As Dr Jiahong Chen explained:

> The real concern here is when data are collected, they can be repurposed for other uses. There is no way we can tell in a smart city what has been collected about us and later what such data may be repurposed for. A lot of the data have been collected initially for well-intended uses, but let us say in some circumstances it could be used for purposes that were not originally envisaged, and there might be unintended consequences. […] That is why we need debate and discussions before we start to build smart cities.[135]

Big Brother Watch provided an illustrative example, stating that "we were concerned by the speed with which the Government funded artificial intelligence cameras and sensors, made by Vivacity Labs, during the pandemic to monitor social distancing in UK towns" and that "very little information was made public about this data processing".[136] This large-scale, invisible processing and unclear accountability poses additional barriers to people exercising their data rights.

55. Third, the operation and processing of data in smart cities brings together many actors, including public and private sector bodies. The ICO has highlighted risks of data sharing, including with law enforcement,[137] and has set out the requirements in several published Opinions (in response to concerns from international organisations and human rights campaigners) for data controllers to mitigate the risks of sharing live facial recognition (LFR) data with law enforcement.[138] Examples of these risks include the inability to exercise any legal rights and freedoms in a public setting (such as privacy rights, data protection rights, freedom of expression, etc), the inability to access services and opportunities, reputational damage, potential discrimination, bias and unfair treatment.[139]

56. The additional risks posed by smart cities represent further issues of relying on individual rights, such as to object or to withdraw consent, in the context of data processing in public spaces. Dr Chen, for example, posited that:

> We are talking about protecting individuals, empowering them, giving them the autonomy, but also if we over-rely on the individual consent we might be shifting the compliance burdens to individual users. That is why I

133 Information Commissioners Office. (TEC0051) para 40
134 Q8; Information Commissioners Office. (TEC0051) para 40; Big Brother Watch (TEC0052) paras 42–4
135 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 13 October 2020, HC (2020–21) 646, Q225
136 Big Brother Watch (TEC0052)
137 Information Commissioners Office (TEC0051) para 40
138 Information Commissioner's Office, *Information Commissioner's Opinion: The use of live facial recognition technology in public places* (18 June 2021)
139 Ibid., p 61

> think there needs to be some technical or legal structure to support people to decide what sort of data are being collected about them and then how they can control the data about them in a way that would respect the fact that they have priorities in life, they have limited energy and attention and time. I think that would be a very big challenge for regulation, but that is something we need to look into in the future.[140]

The ODI's Dr Jeni Tennison further illustrated how the large-scale aggregation of data and profiling of individuals might further undermine individual consent mechanisms:

> An easy example is when you live in a household. Your partner or even your children having consent for data collection from a particular device that you have in your home will affect you as well. If you have multiple people, if lots of middle-class, middle-aged white women like myself give consent for data about them to be collected, that data can also reveal things about myself because I am part of that group, even if I have myself individually withdrawn consent about the collection of that data. Data is not just about us as individuals, they are also about us as families and groups and communities, and also about the whole set of people who are like us and data that they provide can mean that organisations can get insights into us.[141]

57. One way to address the concerns around data rights in smart cities is through data institutions and data intermediaries. "Data intermediaries" refers to a broad category of organisations, with a range of governance models, that facilitate greater access to or sharing of data.[142] The Open Data Institute instead uses the broader term "data institutions", which it defines as "organisations that steward data on behalf of others, often towards public, educational or charitable aims",[143] in order to emphasise the role in collecting, maintaining and sharing data (rather than just facilitating sharing) and the common good (beyond straightforwardly commercial) purposes they can be used for.[144] As Dr Jeni Tennison told us, data institutions "act as this neutral third party to make decisions about how data should be shared and accessed and for what purposes they should be made available".[145] There are several models of data institution/intermediary, including data trusts (which provide fiduciary data stewardship on behalf of data subjects), data co-operatives (where data subjects control the quantity and quality of the data they share), and so on.[146] An article published by the World Economic Forum following the 2022 Davos Agenda noted that data co-operatives complement data protection regimes in Europe and US while also creating economic incentives for participants to share useful, high quality data.[147]

140 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 13 October 2020, HC (2020–21) 646, Q195

141 Ibid.,

142 Centre for Data Ethics and Innovation, *Unlocking the value of data: Exploring the role of data intermediaries* (22 July 2021)

143 Open Data Institute, 'What are data institutions and why are they important?', 29 January 2021

144 Open Data Institute, 'What are data intermediaries?', 18 August 2022

145 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 13 October 2020, HC (2020–21) 646, Q212

146 Centre for Data Ethics and Innovation, *Unlocking the value of data: Exploring the role of data intermediaries* (22 July 2021)

147 "*The key to designing sustainable data cooperatives*", World Economic Forum, 1 February 2022

58. The Government has made some acknowledgements regarding data institutions. The UK National Data Strategy, published in September 2020, sets out five priority areas for Government, including unlocking the value of data across the economy, securing a "pro-growth and trusted" data regime, transforming government's use of data, ensuring the security and resilience of digital infrastructure and "championing the international flow of data".[148] In its response to the consultation on the Strategy, published in May 2021, the Government committed as part of these missions to "bringing about new data institutions and improving the practices of existing ones" in the public, private and third sectors alongside the ODI.[149] The ODI itself notes that many public institutions, like Companies House, the Met Office and the National Archives, already steward data on behalf of citizens, and the Government indirectly supports others by paying to access its services, as the Electoral Commission does with Democracy Club, a Community Interest Company set up in 2010 that collects, aggregates and publishes data scraped from local authorities.[150] The ODI operated three pilot schemes, funded by the Government and Innovate UK, focusing on: data collected in urban spaces (e.g., electric vehicle parking and heating in residential houses); data to help tackle the international illegal wildlife trade; and data on food waste and sales to tackle global food waste. Its report called on policymakers to recognise data stewardship as an appropriate legal purpose, develop guidance on setting up and tools for using data trusts and mandate support, funding and research for data trusts and other types of data stewardship.[151]

59. **Though smart cities provide a range of opportunities, such as more efficient management of resources, there are also additional risks to confidence in privacy and data protection, making it harder for individuals to exercise data rights. *The Government should review how it can incentivise and actively pilot the creation of data institutions, in partnership with local government and other local stakeholders, in smart cities to address issues of data protection and ensure that citizens can have greater control over, and directly participate in the benefits from, the use of their data.***

Workplaces

60. Connected tech is increasingly deployed the workplace just as in the home and city. The development and use of connected tech for the purposes of work such as manufacturing is often conceptualised as part of a "Fourth Industrial Revolution"[152] (4IR or Industry 4.0).[153] Some examples include: product development and manufacturing, using industrial robots, autonomous mobile robots and gateways; logistics and supply chain management, such as sensors feeding data to algorithmic planning processes to reduce costs and inventory waste;[154] and marketing and sales, from customer service chatbots and self-service shops like Amazon's Go and Fresh smart grocery stores, which uses Amazon Dash Carts (infused with cameras and scales to scan items as they are placed in the cart to skip checkouts) and smart speakers to replace shopping

148 Department for Digital, Culture, Media & Sport, *National Data Strategy*, 9 September 2020
149 Department for Digital, Culture, Media & Sport, *Government response to the consultation on the National Data Strategy*, 18 May 2021
150 Open Data Institute, 'How does the UK government currently support data institutions?,' 5 July 2021
151 Open Data Institute, 'Data trusts: lessons from three pilots (report),' 15 April 2019
152 Industry 4.0 is hypothesised to be the next phase in industrial change, following the First (steam power), Second (assembly lines, fossil fuel energy) and Third (telecommunications, computing, data analysis) Industrial Revolutions in the 18th, 19th and 20th Centuries respectively.
153 IBM, 'What is Industry 4.0?', accessed 17 October 2022
154 Qq147, 153, 188

assistants and cashiers.[155] Other, hypothetical examples have also been posited, ranging from automated vehicles revolutionising "last mile" delivery to new "smart factories" of connected machines fully automating production.[156] Connected tech used by businesses and organisations, such as in offices, healthcare and transport, are sometimes referred to as "enterprise IoT" technology (EIOT); connected tech used in industrial settings, like manufacturing, agriculture and energy infrastructure, are often referred to as "industrial IoT" (IIoT). A related term, operational technology (OT), refers to systems that monitor, control and/or adjust physical devices, processes and events in enterprise and industrial operations.

61. The wide range of applications of connected devices in the workplace, from manufacturing, retail and fulfilment and distribution to office work, can bring a wide range of benefits. Dr Asieh Tabaghdehi, Senior Lecturer in Strategy and Business Economics, Brunel University London, argued that connected tech can lead to better and more efficient production, particularly where performance can be optimised through quicker or more proactive workflows, communication and feedback.[157] Amazon illustrated this point by arguing that robotics, machine learning and other technologies in its fulfilment centres had reduced the physical burden on employees, reducing walking time and taking on repetitive tasks, and freed them up to focus on more sophisticated tasks beyond the scope of automation.[158] Connected tech can also be used to empower people traditionally excluded from forms of work: Dr Efpraxia Zamani notes that technologies that facilitate working from home have allowed people with disabilities or living in rural areas secure otherwise-unavailable jobs, albeit with the challenges of developing social relationships at work.[159] Finally, Amazon argued that technology can also improve operational safety, asserting that its global investment worth "hundreds of millions" in "safety improvements across our network spanning state-of-the art safety technology in our vans, driver-safety training programmes, and continuous improvements within our mapping and routing technology" had led to fewer than average instances of injury at work and significant road safety improvements relative to other transportation and warehousing businesses in the UK and US.[160]

62. However, the introduction of connected tech in workplace environments can also have negative impacts on employees. As the ICO notes, "the key difference is the nature of the employer/employee relationship and its inherent power imbalance".[161] Dr Tabaghdehi and Dr Matthew Cole, post-doctoral researcher at the Fairwork Project based at the OII, described to us instances where the micro-determination of time and movement tracking through connected devices, which had been introduced to improve productivity, such as in warehouses had also led to workers feeling alienated and experiencing increased stress and anxiety.[162] Dr Sarah Buckingham similarly described Devon & Cornwall and Dorset Police Services' trial of a "mobile health (mHealth)" intervention, which consisted of giving officers FitBit activity monitors and Bupa Boost smartphone apps to promote physical activity and reduce sedentary time. The trial increased physical activity on average but also led to "feelings of failure and guilt when goals were not met, and anxiety and

155 Q156; see also Amazon, 'Introducing the first Amazon Fresh grocery store', 27 August 2020
156 Q153
157 Q164; see also Dr Ana Canhoto; Professor Ashley Braganza; Dr Asieh Tabaghdehi (TEC0018)
158 Amazon (TEC0065)
159 Q185
160 Amazon (TEC0065)
161 Information Commissioners Office (TEC0051) para 41
162 Qq157–158

cognitive rumination resulting from tracking [physical activity] and sleep".[163] A Report on *Royal Mail* published earlier this year by the then-Business, Energy and Industrial Strategy Committee[164] concluded that data from handheld devices called Postal Digital Assistants (PDAs) had "been used to track the speed at which postal workers deliver their post and, subsequently, for performance management, both explicitly in disciplinary cases and as a tool by local managers to dissuade staff from stopping during their rounds" despite an agreement of joint understanding between Royal Mail and the Communication Workers Union (CWU) in April 2018 to the contrary.[165] The Report subsequently invited the Information Commissioner "to review the legal basis for the collection, storage and use of this data and to report their findings to the Committee".[166] Dr Cole also argued that, more broadly, technological transformation would likely lead to a change in task composition and a deskilling of many roles as complex tasks are broken up into simpler ones to allow machines to perform them.[167] Dr Tabaghdehi cited the education sector as one profession likely to experience disruption due to technological transformation.[168]

63. Despite these effects, there are often few options for recourse amongst employees. As Dr Cole told us:

> One of the biggest issues concerns control over data, as the other people mentioned. GDPR provides a certain degree of protection for private individuals. However, it is more limited in protecting workers in the workplace. There are a few provisions there that specifically deal with subject-access requests and protect workers against algorithmic decision-making, like hiring and firing purely by algorithm, but there is a lack of enforcement.
>
> Unless there is a union that is litigating around these things or an existing collective bargaining agreement, there is a lack of enforcement at the state level. The UK Government could do much better at ensuring protections for worker data and protecting citizens of the UK from global giants like Uber, for example. It is one of the most visible ones, but there are many other less visible players that contribute to the data broker economies.[169]

The ICO had noted that respondents to a recent call for evidence on employment practices "raised concerns around the use of connected tech in workplace scenarios including the increased use of monitoring technologies, as well as the ways in which AI and machine learning are impacting how decisions are made about workers" and said it "will provide more clarity on data protection in the employment context as part of this work".[170] Dr Cole also called for greater observation and monitoring of AI system deployments, empowered labour inspectorates and a greater role for the Health and Safety Executive (HSE), the UK regulator for workplace health and safety, in regulating workplace AI systems and upholding standards of deployment.[171]

163 Dr Sarah Buckingham (TEC0014)
164 The Committee is now the Business and Trade Committee (since 16 April 2023), following the aforementioned machinery of government changes that similarly impacted our remit.
165 Business, Energy and Industrial Strategy Committee, Seventh Report of Session 2022–23, *Royal Mail*, HC 1045, paras 7–13
166 Ibid., para 17
167 Qq164–166
168 Qq167–168
169 Q156
170 Information Commissioners Office (TEC0051) para 44
171 Q183

64. **The monitoring of employees in smart workplaces should be done only in consultation with, and with the consent of, those being monitored.** ***The Government should commission research to improve the evidence base regarding the deployment of automated and data collection systems at work. It should also clarify whether proposals for the regulation of AI will extend to the Health and Safety Executive (HSE) and detail in its response to this report how HSE can be supported in fulfilling this remit.***

65. ***The Information Commissioner's Office should develop its existing draft guidance on "Employment practices: monitoring at work" into a principles-based code for designers and operators of workplace connected tech.***

Data Protection Reform

Data adequacy and international harmonisation

66. Because connected tech is manufactured by multinational companies and can often utilise cloud services that are hosted and process data in different jurisdictions, it is important that data rights are held to the same standard wherever that data may be processed. Data adequacy refers to the (ongoing) assessment process regarding whether or not the data protection in one jurisdiction over data about citizens of a second jurisdiction is essentially equivalent or compatible to the data protection in the second jurisdiction.[172] The term is typically used by the European Union to describe other jurisdictions with whom it permits cross-jurisdictional flows of personal data following a technical and legal assessment process.[173] The EU formally recognised the UK's data protection regime in an adequacy decision published on 28 June 2021.[174]

67. However, the Government has also consistently stated that it would pursue what it described as "a pro-growth and trusted data regime" in the context of an increasingly connected and digitised world.[175] The National Data Strategy, published in September 2020 (prior to the adequacy decision), asserted that the Government would "maintain and bolster a data regime that is not too burdensome for the average company" and cited the need for "a data regime that is neither unnecessarily complex nor vague" while also "championing the international flow of data".[176] In September 2021, the Government launched a consultation on data protection reform, which it stated would "deliberately build on the key elements of the current UK General Data Protection Regulation (UK GDPR), such as its data processing principles, its data rights for citizens, and its mechanisms for supervision and enforcement".[177] The June 2022 UK Digital Strategy indicated that these reforms would be enacted through primary legislation[178] and the Government introduced the Data Protection and Digital Information Bill the following month.[179] The Bill was subsequently paused following ministerial changes throughout autumn 2022 and was

172 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 13 October 2020, HC (2020–21) 646, Qq205–10

173 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 26 January 2021, HC (2020–21) 646, Q267

174 "*EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK*", Department for Digital, Culture, Media & Sport press release, 28 June 2021

175 Department for Digital, Culture, Media & Sport, *National Data Strategy*, 9 September 2020

176 Ibid.

177 Department for Digital, Culture, Media & Sport, *Data: a new direction*, 10 September 2021

178 Department for Digital, Culture, Media & Sport, *UK Digital Strategy*, 13 June 2022

179 Data Protection and Digital Information Bill

eventually reintroduced as the Data Protection and Digital Information (No. 2) Bill in March 2023 after the machinery of government changes the previous month.[180]

68. Both the former and current Information Commissioners have given their perspectives on international harmonisation and adequacy in the context of discussing the future of the data protection framework. The previous Information Commissioner, Elizabeth Denham, cited broad international trends when arguing in favour of the GDPR approach before our Sub-Committee on Online Harms and Disinformation in 2021:

> I think the advantage of the GDPR approach is that other countries around the world are using GDPR as a model to reform their law, so the direction of travel and the trajectory of where the laws are going is to give people stronger rights. GDPR gets a bad rap from people who say it is just about the paperwork of privacy or having to record all your decisions around data. We are trying to bust that myth because, at its heart, data protection is about respect for customers' and citizens' data and about individuals having the right of agency around their personal data.
>
> It is more important for the reputation of Governments and businesses than it has ever been. We talked a minute ago about millions of users abandoning WhatsApp because they are concerned about data and the terms of service. It is so important that Government, in their policy, take people with them and there is trust and confidence in the digital economy. Stripping down GDPR to its main principles, it is about protection of individuals and certainty for business, and knowing what they are supposed to do to account for data.[181]

Current Commissioner, John Edwards, similarly cited data adequacy as a key priority for the ICO regarding data protection reform:

> I have been very pleased to be engaged with Government in looking at their reforms and from the outset my position was that I would like to see these reforms get to a position where I am in a position at the ICO to publicly support them. That means ensuring that none of the proposals reduce the rights of people in the United Kingdom; that the proposals do not put in peril the adequacy determination with the EU; and that the reforms allow me as regulator to make compliance easier and to reduce the cost of compliance for businesses in the UK.[182]

69. The Minister posited that "one of the key objectives" of data protection reform has been to maintain adequacy, but also cited the ambition to build so-called "data bridges" with other countries.[183] She explained that:

> Some companies do not transfer a great deal of data internationally, and it will give them more flexibility. We are trying to be more proportionate in the approach that we take, so that we are not pulling in lots of smaller businesses with lots of compliance and regulations that they do not fully

180 Data Protection and Digital Information (No. 2) Bill
181 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 26 January 2021, HC (2020–21) 646, Q267
182 Q285
183 Q372

> understand. We are trying to give scientific researchers more flexibility in how data is shared, so that they can have more bandwidth to do research activities. As I say, it is an evolution rather than revolution.
>
> We think that, as they develop, some of the key technologies will require more flexibility than GDPR allows. We are trying to gradually step away from the very restrictive processes that are under the GDPR, and also to try to build more flexible relationships with international partners whom we trust, so that businesses are able to transfer data internationally to more partners. The adequacy process under the EU can be quite lengthy, and we think that we can be more agile in terms of building the partnerships we need with key international economies going forward. We are just trying to create that agility and flexibility over a period of time, rather than have some great revolution where we suddenly break free of the GDPR system.[184]

The Minister has since confirmed, in response to further questions about the possible loss of data adequacy and the cost to businesses and scientific research, that the Government has "been in constant contact with the European Commission about our proposals […] to make sure that there are no surprises".[185]

70. Despite these ambitions, none of the stakeholders we engaged called for reform to data protection legislation. Indeed, several academics and campaigners have argued in favour of preserving equivalent levels of data protection with Europe.[186] Big Brother Watch was most robust in its argument, stating that "in our view, the data 'reform' plans set the Government on a perilous journey which threatens data adequacy, international privacy standards and rights protections for everyone in the UK".[187] Since our inquiry concluded, it has been reported that Ireland's Data Protection Commission has fined Meta a record €1.2 billion (£1 billion) and ordered the company to suspend the transfer of user data from the EU to the US, after finding that it did so without proper safeguards in place.[188]

71. Contributions from the tech sector itself did not agitate for significant data protection reform and instead highlighted the importance of universal standards. While techUK has elsewhere since supported the Government's plans for data reform,[189] in evidence to our inquiry it characterised the UK's pre-existing data protection regime as "an example of robust regulation" and "generally well understood and effectively enforced", instead calling for closer attention by the ICO in helping SMEs with "the right support, resources and guidance".[190] AMDEA, the Association of Manufacturers of Domestic Appliances, simply described the Government's ambition "to shape an accessible interoperable international data ecosystem in order to harness the power of responsible data and promote growth" as "welcome principles for the upcoming Data Reform Bill".[191] Google's David Kleidermacher demurred from giving direct thoughts on the impact of data protection reform on data

184 Q373
185 HC Deb, 17 April 2023, col 70 [Commons Chamber]
186 Qq8, 68; Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); Horizon Digital Economy Institute, University of Nottingham (TEC0046); Big Brother Watch (TEC0052); see also *Data Protection and Digital Information (No. 2) Bill*, Research Briefing CBP-9746, House of Commons Library, March 2023
187 Big Brother Watch (TEC0052) para 71
188 "*Facebook owner Meta fined €1.2bn for mishandling user information*", The Guardian, 22 May 2023
189 "*Plans to reform the UK's data protection regime represent an important evolution for the UK GDPR*", techUK press release, 17 June 2022
190 techUK (TEC0049); see also Q16
191 AMDEA (TEC0056)

adequacy, but advocated for harmonisation in general:

> [C]ertainly having harmonised standards is very helpful. This is feedback that we have provided to DCMS for years now around the code of practice for security and now with the app store code of practice discussion. A big part of our feedback, especially for small and medium-sized businesses, is that having harmonised standards is really important. If every country has a different set of rules, that makes it very difficult cost-wise to keep up.[192]

Amazon's Leila Rouhi likewise argued that "certainly I think that consistency and unambiguous regulations are necessary, if not incredibly helpful for us—ultimately, our aim is to ensure that we can continue providing a seamless and consistent customer experience and we know how to achieve that while also being compliant with the law".[193] Even under the current regulatory framework, the UK in 2022 became only the third country behind the US and China to have a tech sector to have a total valuation of $1 trillion, with more high growth start-ups and venture capital investment than European peers.[194]

72. **The Government has not yet made a compelling case for reform of data protection. While we understand that some companies do not share data outside the UK, we are concerned that differing expectations between those companies and companies that do share data outside the UK may give the impression of "lesser" protections for processing personal data in the UK overall. This could be perceived as undermining our existing data adequacy arrangements and ultimately harm companies that share data between the UK and other jurisdictions. *To maintain the UK's reputation as a world-class technology hub, the Government should keep its data reforms under review so as not to undermine its existing data adequacy agreements.***

Reform of the Information Commissioner's Office

73. The Data Protection and Digital Information (No. 2) Bill proposes a range of reforms to the structure, governance and role of the ICO. The ICO is currently structured as a "corporation sole", which is a single legal entity created by statute consisting of an incorporated office occupied by a single person.[195] This means that the ICO does not have a chair and statutory independent board that provides direction and structure of its executive function, unlike most of its peer regulators.[196] The Government has asserted that "this model can lead to a lack of diversity, challenge and scrutiny that is critical to robust governance and decision-making".[197] The Bill will therefore replace the ICO with a body corporate called the Information Commission,[198] run by a chief executive and with the "Information Commissioner" title attached to the role of chair, to bring the regulator in line with other bodies of comparable size and remit such as Ofcom and the Financial Conduct Authority.[199] The Bill's explanatory notes argue that "the nature of the regulator's

192 Qq343–344
193 Q345
194 "*UK tech sector retains #1 spot in Europe and #3 in world as sector resilience brings continued growth*", Department for Digital, Culture, Media & Sport press release, 21 December 2022
195 *Data Protection and Digital Information (No. 2) Bill*, Research Briefing CBP-9746, House of Commons Library, March 2023, p 46
196 Department for Digital, Culture, Media & Sport, *Data: A new direction*, 10 September 2021, pp 123–4
197 Ibid., p 124
198 Data Reform and Digital Information (No. 2) Bill, Clauses 100–103
199 Department for Digital, Culture, Media & Sport, *Data: A new direction*, 10 September 2021, p 124

role and responsibilities remains fundamentally unchanged".[200]

74. The Government's legislative proposals also provide further reforms to the ICO in several areas. These include the introduction of "statements of strategic priorities set by the Government,[201] requirements to consult stakeholders when considering how the exercise of its functions might affect economic growth, innovation and competition, such as regarding issues relating to emerging technology[202] and powers for the Secretary of State to reject codes of guidance on processing personal data (after which the Commissioner must revise the code and resubmit to the Secretary of State for approval).[203]

75. The response from civil liberties organisations to the breadth of reforms has been at best mixed throughout the process. In its consultation response to proposals, the Government noted majority support for measures including a new overarching statutory objective, a new duty to consult and co-operate with other regulators, strengthened reporting and impact assessment requirements, enhanced enforcement powers and a more efficient complaints handling framework.[204] However, it also acknowledged that the majority of respondents disagreed with proposals to give the Secretary of State powers to make statements of strategic priorities and to approve codes of practice and guidance on the basis of the risk to the ICO's independence, and that there was only a plurality of agreement to proposals for a new statutory framework, reform of the governance and appointments processes and the requirement to appoint expert panels for the same reason.[205] Most recently, a group of 26 civil society organisations wrote to the Secretary of State for Science, Innovation and Technology critiquing the Bill's provisions to give the Government the power to "issue instructions and interfere with the regulatory function of the [ICO], […] which is particularly problematic as the ICO plays a key role in oversight of the government's use of data".[206]

76. When we raised the impact of reforms on the ICO's independence with the Minister, she responded that "the main person that it is important has confidence in the reforms is the Information Commissioner himself" and said that she has "discussed the proposals about adding a level of Secretary of State power in this regard".[207] She also noted, in response to a question about the lack of support in the consultation for the breadth of reforms, that:

> I think some of the concerns in relation to the Secretary of State's role on strategic direction of the ICO have been slightly overblown. That is evidenced by the fact that the Information Commissioner himself is comfortable with the place that this has landed. It is something that I have discussed with him throughout, because I think having his support for our reforms throughout this process is incredibly important.[208]

200 Explanatory Notes to the Data Protection and Digital Information (No. 2) Bill [Bill 265 (2022–23) —EN]
201 *Data Protection and Digital Information (No. 2) Bill*, Research Briefing CBP-9746, House of Commons Library, March 2023, p 49
202 *Data Protection and Digital Information (No. 2) Bill*, Research Briefing CBP-9746, House of Commons Library, March 2023, pp 48–9
203 Ibid., Clause 31
204 Department for Digital, Culture, Media & Sport, *Data: a new direction - government response to consultation*, 23 June 2022
205 Ibid.
206 Open Rights Group, *Open letter to Rt Hon Michelle Donelan MP* (7 March 2023)
207 Qq411–2 [Julia Lopez]
208 Q412

77. The introduction of new powers for the Secretary of State mirrors the debate about equivalent powers provided by the Online Safety Bill over the online safety regulator Ofcom. We raised similar concerns in our scrutiny of the Draft Online Safety Bill[209] and the iterations of the Bill that have been introduced to Parliament[210] that those powers for the Secretary of State to reject codes of practice for online safety may undermine the independence of the regulator. Indeed, William Perrin, Trustee of the Carnegie UK Trust, argued that those powers delegated to the Secretary of State in the Online Safety Bill, as have been replicated in the Data Protection and Digital Information (No. 2) Bill, were:

> explicitly drafted so that the Secretary of State can infinitely reject proposals it receives from Ofcom until it gets the proposal it wants. It is a very unusual power and that is before the Secretary of State then brings the [Statutory Instrument] to Parliament.[211]

Dr Edina Harbinja, Senior Lecturer at Aston University, likewise told us that the powers in the Online Safety Bill made her "fear that [the regulator's] independence may be compromised" and that "similar powers are creeping into other law reform pieces and proposals, such as the data protection proposal".[212] We explicitly recommended at the time that the Government remove these powers from the Bill and called on it to "maintain its approach to ensuring independent, effective and trustworthy regulation that has a proven track record in other sectors".[213] Despite our consistent criticism, the Government has continued with its intention to provide these powers to the Secretary of State in its legislative proposals in both online safety and data protection reform.

78. **We agree that reforming the governance and accountability structures of the Information Commissioner's Office will be a positive step.** ***We have previously recommended against executive overreach in the case of Ofcom and the Online Safety Bill; these concerns apply with respect to the Information Commissioner's Office and the Data Protection and Digital Information (No. 2) Bill. Powers to veto codes of practice and to set strategic priorities without parliamentary oversight should not be adopted.***

209 Digital, Culture, Media & Sport Committee, Eighth Report of Session 2021–22, *The Draft Online Safety Bill and the legal but harmful debate*, HC 1039, para 29

210 Digital, Culture, Media & Sport Committee, First Report of Session 2022–23, *Amending the Online Safety Bill*, HC 271, paras 3–6

211 Ibid., para 4

212 Ibid., para 3

213 Ibid., para 6

2 Product security

79. Connected devices can enhance their functionality by communicating with networks of other devices and accessing additional storage and processing power through cloud and/or edge computing. However, this connectivity also exposes them to security breaches, cyberattacks and cybercrime. As people and organisations become more reliant on digital technologies, including connected tech, the risks and potential impacts of cyberattacks also increase. These attacks can invade users' privacy, create malfunctions and even cause financial and material harm by stealing bank credentials and enabling fraud.[214]

80. Individuals, organisations and governments all need to take measures to protect their connected devices and mitigate the risks and impacts of cyberattack. There are several important concepts that describe these measures. "Cyber resilience" refers to the ability for organisations to prepare for, respond to and recover from cyberattacks.[215] "Cybersecurity" refers to the practice of protecting devices, systems, services and information from attack; many companies offer a range of products and services to help improve cybersecurity.[216] "Cyber hygiene", a related term, refers to the regular, precautionary steps that individuals and organisations can take, like changing passwords, updating software and scanning for viruses, to mitigate the risk and impact of breaches.[217]

Cybersecurity of connected tech

Cyber threats

81. Any connected device, network or system may be vulnerable. Specific vulnerabilities are known as "attack vectors"; the sum total of a device, network or system's attack vectors is referred to as the "attack surface".[218] As connected devices proliferate across all domains in society, the total attack surface is also increasing, creating more opportunities for threat actors. Professor George Loukas, Professor of Cyber Security and Head of the IoT and Security (ISEC) Research Centre at the University of Greenwich, warned that the increasing attack surface might exacerbate the threat of cyberattack across society:

> What is happening is that, through digital transformation across all sectors, we have opened ourselves to vulnerabilities across every domain and in every little system: from the mobile device to the connected device, the computer, every little app we use, social media, cloud and so on. Because there is such a large attack surface, it makes sense that there will be many people who will successfully—by chance, perhaps—find that this is the way that it works.[219]

82. Official statistics show that cyberattack poses a significant, yet underappreciated, material risk to the public.[220] Connected tech presents an appealing target because

214 Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (7 March 2018), p 6
215 Department for Science, Technology & Innovation and Department for Digital, Culture, Media & Sport, 'Cyber resilience', accessed 12 May 2023
216 IBM, 'What is cybersecurity?', accessed 12 May 2023
217 Microsoft, 'How to Have Better Cyber Hygiene', 8 July 2022
218 IBM, 'Anatomy of an IoT malware attack', 7 August 2019
219 Q116
220 National Cyber Security Centre, NCSC Annual Review 2022, 1 November 2022

cybersecurity for devices is often less robust, often overlooked and updated or patched less frequently. The Government's impact assessment for the Product Security and Telecommunications Infrastructure (PSTI) Bill warns that "the estimated cost to the consumer, from insecure consumer IoT alone, over the next ten years is £14.8 billion".[221] A 2020 report from cybersecurity solutions company Palo Alto Networks on the cybersecurity threat to connected devices, based on analysis of over a million devices in thousands of physical locations, found that 57 percent of connected devices are vulnerable to medium- to high-severity attacks and 41 percent of cyberattacks exploit device vulnerabilities, as attackers scan through connected devices in an attempt to exploit known weaknesses.[222] Public services may also be particularly vulnerable. Palo Alto Networks' research on connected tech in healthcare found that over 98 percent of all connected device traffic was unencrypted.[223]

83. Similarly, private sector organisations are under constant cyberattack. The Government has found that 39 percent of businesses identified cyberattacks in 2022, consistent with previous years, and that 31 percent of businesses and 26 percent of charities estimated that these attacks occurred at least once a week.[224] Google's David Kleidermacher discussed the extent of the challenge of cyber threats facing businesses in particular:

> At Google, given the scale of the services and products that we offer across the world and given that literally every single day, in fact as we sit here right now, we are under constant cyberattack. We have a very strong economic incentive, and have had that for many years now, to invest and be proactive about cybersecurity. For many businesses, until you have been attacked, which many of them have not been yet, they are going to be reactive because there are plenty of other things to worry about and prioritise in order to make their profits.[225]

84. The attacks have material impacts on the private sector. One in five businesses and charities say they experienced a negative outcome as a consequence of a cyberattack.[226] DCMS estimates that, on average, the business cost of cyberattacks was £4,200 per year, rising to £19,400 when considering only medium and large businesses.[227] While these numbers are in and of themselves stark, the Government has also warned that many consumers and "less cyber mature" businesses either may not know that they have been hacked and/or may be underreporting.[228]

Threat actors

85. Cyberattacks are perpetrated by a range of people and individuals, referred to as "threat actors" or "malicious actors". Threat actors may have a range of motivations, including surveillance, espionage, retribution, financial gain and influence operations.[229]

221 Department for Digital, Culture, Media and Sport (TEC0054) para 8
222 Palo Alto Networks, *2020 Unit 42 IoT Threat Report*, 10 March 2020
223 Ibid.
224 Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey 2022*, 11 July 2022
225 Q364
226 Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey 2022*, 11 July 2022
227 Ibid.
228 Department for Digital, Culture, Media and Sport (TEC0054) para 8; see also Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey 2022*, 11 July 2022
229 Q74; see also Microsoft, 'How Microsoft names threat actors', 20 April 2023

86. The National Cyber Security Centre (NCSC), the UK agency charged with providing expertise, advice and incidence response to cyber threats in support of the wider public sector, private sector and general public, assesses that the most consistent, sophisticated and ambitious global threat actors are China and Russia, followed by Iran and North Korea.[230] Nation-states typically conduct stealthy, multi-year campaigns with various levels of intrusion.[231] During our inquiry, we heard that the targets of state intrusion are not only other states, but the private sector and households too. Google's David Kleidermacher noted that "we [Google] are under constant attack and one of those areas is state-sponsored attack and threats, including from China".[232] NCC Group's Matt Lewis explained that "we also know that, through groups like Lazarus and others, some nation states—North Korea—have been attributed with ransomware attacks where they use those as a legitimate means of financial gain".[233] During our visit to South Korea, we heard how the country is constantly at risk of cyberattack from North Korea and that North Korean state actors and state-affiliated attackers have pivoted from attacking state and critical national infrastructure to households, ranging from malware (such as ransomware) attacks to leaking and exposing sensitive information online. In response, South Korea has aimed to both revise its domestic response[234] and strengthen international co-operation, particularly with the United States, in recent years.[235] The Government's own National Cyber Strategy 2022 has affirmed its ambition for "the UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals".[236]

87. Beyond state actors, threat actors may include organised criminal gangs, terrorists and hackers.[237] In its own taxonomy of threat actors, multinational tech company Microsoft also lists "private sector offensive actors" (or PSOAs), which are "commercial actors that are known/legitimate legal entities, that create and sell cyberweapons to customers who then select targets and operate the cyberweapons" that "threaten many global human rights efforts" such as by "targeting and surveilling dissidents, human rights defenders, journalists, civil society advocates, and other private citizens".[238] When asked whether state actors remained the most capable threat actors in the threat landscape, Palo Alto Networks' Simon Moore observed that:

> I think there is a blurring now. They will be supporting organised crime agencies, or the people who are in those will flow to and fro between them.[239]

88. Finally, some threat actors may simply be random individuals. As Mr Lewis explained:

> We even have what we might call the bedroom hackers, or the "script kiddies"[240], who, for whatever reason—just out of fun or for curiosity—can

230 National Cyber Security Centre, *Annual Review 2021* (17 November 2021) p 19
231 Q74
232 Q367
233 Q74
234 So Jeong Kim and Sunha Bae, "*Korean Policies of Cybersecurity and Data Resilience*", *The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way*, Carnegie Endowment for International Peace (17 August 2021)
235 "*The Future of South Korea-US Cyber Cooperation*", The Diplomat, 14 October 2022
236 HM Government, *National Cyber Strategy 2022* (15 December 2021) p 11
237 Q74; see also Security Service, 'Cyber', accessed 4 May 2023
238 Microsoft, 'How Microsoft names threat actors', 20 April 2023
239 Q108
240 Unskilled actors using pre-made programs for malicious purposes.

> cause sometimes quite significant damage going after certain organisations when they find a loophole, manage to identify a data breach, and maybe publicly dump that and expose the business in the process.[241]

Indeed, the 2016 Mirai botnet attack, which infiltrated hundreds of thousands of connected devices and used them to disrupt internet infrastructure and services including the BBC and Netflix for several hours, was perpetrated by a Rutgers undergraduate student and two university-aged friends.[242]

Cyber risks

89. The Government delineates three broad types of risk that must be mitigated:

- **Consumer risk**, caused by people buying insecure devices and/or not knowing how to protect themselves from cybercrime, and manufacturers not becoming aware of and/or addressing cybersecurity vulnerabilities;
- **Enterprise risk**, caused by a lack of cyber resilience across the wider economy, a lack of clarity on how to monitor and/or protect against cybercrime, and differing baseline expectations for product security due to a lack of alignment in international standards; and
- **Risk to critical national infrastructure** (CNI), due to the critical importance and essentiality of such services to society combined with the relatively low-cost nature of cyberattack relative to other forms of attack.[243]

90. The risk of cyberattack can be difficult to quantify until it is experienced first-hand. As Professor Loukas asserted:

> What there is a doubt about is whether [people] know the level of risk. With social media, for example, we have some idea about the level of risk. We have heard so many things, and we interact. Most people—most parents, even—will know, for example, how to advise their kids on social media. With emails and websites, we have some experience by now. It has been decades, and we know what might look okay and what might not look okay.
>
> When it comes to connecting to devices, in all our research and in research that we have seen from other universities, people do not know the risks. They simply do not know the risks. They either choose to ignore them because it is often convenient to ignore risks, or they exaggerate risks. They might consider a completely different risk. Something that has never happened, for example, is a serious risk, and they might not consider something that is happening every day. The big change happens the moment you are hacked or when someone you know is hacked.[244]

Indeed, the nature of connected devices means that many people may not realise that a device or system has been compromised. As Simon Moore explained, "it is really hard to

241 Q74
242 Q108; Department for Digital, Culture, Media and Sport (TEC0054) para 10; "*How a Dorm Room Minecraft Scam Brought Down the Internet*", Wired, 13 December 2017
243 Department for Digital, Culture, Media and Sport (TEC0054)
244 Q104

identify it because there is no telemetry, and there are not that many indicators on the box […] it is not like your PC or even your phone, which will give you an alert".[245]

91. Often, cyberattacks may be crimes of opportunity rather than calculated against specific targets. Simon Moore speculated that targets were generally picked at random:

> Basically, they go fishing—looking—for someone who has a known vulnerability. If we take [operational technology], for example, if you have bought a baby camera or nursery camera that has a breach on it, they will go looking for it. They will look across the entire market—the entire globe—and when they have found it, they will go, "right, that is my pivoting point."[246]

Evidence from consumer advice organisation Which?, noted that "cybercrime is often incorrectly viewed as a 'victimless' crime" despite "the potential to ruin livelihoods, and cause severe personal distress".[247]

Box 2: Common types of cyberattack

Physical attacks or tampering, where an attacker accesses an unattended or insecure physical device (e.g., with an "evil maid attack", where an attacker installs a malicious bootloader and gains access to the device when it next boots up);

Phishing, where an attacker poses as a trusted actor to obtain sensitive information;

Malware, such as spam bots (which use the device to relay spam messages), brickers (destructive malware that make devices unusable) and ransomware (which lock down access to files and devices to extort a ransom in exchange for the decryption key);

Brute-force password attacks, where an attacker submits many passwords (usually in an automated process) with the intention of correctly guessing the user's password and gaining access to the system;

Software and firmware hijacking, which targets devices with out-of-date software and firmware (i.e., software that controls the physical device itself), including "zero-day attacks", which target devices with software vulnerabilities on release before manufacturers can patch them;

Information disclosure/eavesdropping, where an attacker intercepts network traffic without authorisation, **encryption attacks**, where an attacker circumvents encryption systems, and **Man-in-the-middle attacks**, where attackers intercept and modify communications;

Denial of service (DoS) and distributed denial of service (DDoS) attacks, which aim to overwhelm a device or system with traffic to make it unavailable (such as by using a "botnet", an aggregation of individual bots, programs or devices, controlled by a single person to perform tasks in concert); and

IoT botnet attack, such as the "Mirai attack", where an attacker creates a botnet from hacked connected devices in order to execute a DDoS attack elsewhere.

Sources: Qq87, 94, 107; Cisco, 'What Is a Cyberattack?', accessed 4 May 2023; Microsoft, 'What is a cyberattack?', accessed 4 May 2023

245 Q69
246 Q72
247 Which? (TEC0045) para 9

Types of cybercrime

92. There are many different and evolving ways that an attacker may attempt to compromise a connected device. Of these cyberattacks, 83% were phishing attempts (where an attacker attempts to trick a user into divulging sensitive information). However over 20% of the affected businesses identified more sophisticated attacks such as denial of service, malware or ransomware. Cyberattacks can therefore range from low sophistication, high-frequency attacks to high sophistication, high-impact attacks and are likely to involve an element of human deception or mistake to gain access to a system.[248] Cyberattacks may also attempt to exploit different weaknesses in the various layers of the tech stack (see paragraphs 6 and 7), from the device itself via its hardware or software or through the wider systems in which it interoperates, such as its networks, servers, cloud platforms and applications and websites that it may access in order to function.[249]

Improving device security

Secure by Design and the product security regime

93. During this Parliament, the Government has aimed to improve cybersecurity for consumer devices through its Product Security and Telecommunications Infrastructure (PSTI) Bill. The origins of the product security regime can be traced back to the Government's "secure by design" framework, which was initiated as part of the Government's cybersecurity ambition as part of its National Cyber Security Strategy 2016–21.[250] The framework culminated in a voluntary Code of Practice, published in October 2018, that was applicable to "consumer IoT products" that "are connected to the internet and/or home network and associated services".[251] The Code established 13 guidelines, including no default passwords, vulnerability disclosure policies (i.e., a public point of contact for researchers and others to report issues that "should be acted on in a timely manner") and software updates (with clear end-of-life policies and minimum support periods, clear reasonings and easy-to-implement updates).[252] Other guidelines[253] cover secure data and communications, data protection measures, simple installation and maintenance and minimising attack surfaces. The Code subsequently set the international standard for cybersecurity of commercially available connected devices: in February 2019, the European Telecommunications Standards Institute (ETSI), a European Standardisation Organisation that supports the development of technical standards for information technology systems, published its baseline requirements for consumer IoT[254] based on the UK Code of Practice's 13 guidelines.[255]

248 Q87
249 Q94
250 Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (7 March 2018), p 10
251 Department for Digital, Culture, Media & Sport, *Code of Practice for Consumer IoT Security* (October 2018), p 5
252 Ibid., pp 6–17
253 In full, the other ten guidelines are: securely stored credentials and security-sensitive data; secure (i.e., encrypted) communications; minimise exposed attack surfaces; ensure software integrity (e.g., alerting consumers to unauthorised changes); ensure personal data is protected; make systems resilient to outages; monitor system telemetry data (i.e., on usage and measurements, to help identify anomalies); make it easy for consumers to delete personal data; make installation and maintenance easy (i.e., with minimal steps, guidance and following best practice on usability); and validate input data (i.e., ensure data inputs are properly formed, to prevent malfunctions occurring in other components).
254 European Telecommunications Standards Institute, '*EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements*', accessed 9 May 2023
255 "*Government to strengthen security of internet-connected products*", Department for Digital, Culture, Media & Sport and National Cyber Security Centre press release, 27 January 2020

94. Despite its preference for self-regulation, and in response to industry stakeholder and expert feedback regarding the risk to individuals and the wider economy, the Government launched a consultation on options for making the Code of Practice mandatory.[256] In February 2020, following the December 2019 General Election, the Government confirmed that it would aim to achieve full market compliance with the most important guidelines as "the first practical step towards more secure devices".[257] The Government launched a consultation on its legislative proposals in July 2020 and updated its policy intentions in response to feedback in April 2021.[258]

95. The Product Security and Telecommunications Infrastructure (PSTI) Bill was introduced on 24 November 2021. The Bill's explanatory notes explained that the main impetus for legislating was the fact that voluntary compliance with the 2018 Code of Practice "was slow" and "poor security practices remain commonplace"; for example, the Internet of Things Security Foundation estimated that, following the Code's publication, the proportion of manufacturers maintaining an adequate disclosure programme had only increased from 9 percent in 2018 to 13 percent in 2019.[259] The regime's relevant measures will aim to:

- Codify the three top guidelines from the Code of Practice, namely regarding banning default, universal passwords, introducing vulnerability disclosure policies and creating transparency about software updates
- Provide Ministers with powers to add and amend minimum security standards;
- Require manufacturers, importers and distributors to comply with duties in relation to the security requirements; and
- Create an enforcement regime with civil and criminal sanctions aimed at preventing insecure products being made available on the UK market.[260]

Erika Lewis, Director of Cyber Security and Digital Identity at DSIT (formerly at DCMS), explained the ambitions of the Bill:

> The route that we went down with the PSTI Bill was not putting the consumer or the citizen in a position where they have to think through that basic level of security, because in the future, when that is in force, the product won't have a default password, so one of these factory passwords. The consumer will know how long the software on the product will be updated for and there will be somewhere that they can contact in terms of a vulnerability.[261]

256 Department for Digital, Culture, Media & Sport, *Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security*, 1 May 2019

257 Department for Digital, Culture, Media & Sport, *Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation*, CP 213, 27 January 2020

258 Department for Digital, Culture, Media & Sport, *Government response to the call for views on consumer connected product cyber security legislation*, 21 April 2021

259 Explanatory Notes to the Product Security and Telecommunications Infrastructure Bill [Bill 199 (2021–22) —EN]; see also Dr Leonie Tanczer (TEC0021)

260 Department for Digital, Culture, Media & Sport, Factsheet 1 - Overview of the Product Security and Telecommunications Infrastructure (PSTI) Bill, 1 December 2021

261 Q386

The regime will be enforced by the Office of Product Safety and Standards (OPSS), the UK regulator for consumer product safety and measurement standards.[262] The Bill received Royal Assent on 6 December 2022.[263] Businesses will be given time to adjust their practices before the regime comes into force.[264]

Perspectives on the product security regime

96. Contributors to our inquiry consistently described the requirements of the regime as an important "first step" in improving consumer cybersecurity. Sarah Turner, a doctoral researcher at the University of Kent, and Dr Jason Nurse, Senior Lecturer in Cyber Security at the University of Kent and Public Engagement Lead at Kent Interdisciplinary Research Centre in Cyber Security, have found that it was impossible to rely on users to ensure devices were set up properly due to a lack of robust, easy-to-follow guidance, the lack of prompting to review default security arrangements, the perspective that connected devices were not "'serious' elements in their homes" and the lack of seamless interoperability and baseline security between different types and brands of device.[265] They therefore conclude that:

> incorporating the remaining steps in the DCMS Code of Practice for Consumer IoT Security […] in any future legislation would add significantly to the safety of users, if only by raising the bar to entry for potential producers in requiring the production of more secure and robust devices. Our research suggests that users do not understand the devices they are using sufficiently to ensure their own safety, meaning that the most appropriate way to mitigate risk to users would be through additional robust regulatory and legislative measures.[266]

Dr Cigdem Sengul of Brunel University London similarly argued that "establishing good security and privacy defaults, in general, is a good measure, as end-users may not follow all recommendations, finding them cumbersome".[267]

97. However, these same submissions, from academics in the field, as well as the Government-funded UKRI Trustworthy Autonomous Systems Hub, also consistently argued that the Bill did not go far enough in codifying best practice for manufacturers, importers and distributors.[268] Written evidence from Which? argued, with reference to the 2018 Code of Practice, that "it is critical that this legislation remains flexible to ensure further security principles can be adopted over time".[269] The Horizon Digital Economy Institute at the University of Nottingham called for regulatory sandboxes and guidance in following the 2018 Code to support industry and enhance the reputation and competitiveness of British products in European and global markets.[270]

262 Q420
263 Product Security and Telecommunications Infrastructure Act 2022, Introductory text
264 *The Product Security and Telecommunications Infrastructure Bill*, Briefing Paper CBP9430, House of Commons Library, 25 October 2022
265 Sarah Turner; Dr Jason Nurse (TEC0029)
266 Ibid.
267 Dr Cigdem Sengul (TEC0016) para 4.2
268 Dr Cigdem Sengul (TEC0016); Dr Leonie Tanczer (TEC0021); Sarah Turner; Dr Jason Nurse (TEC0029); Dr Subhajit Basu (TEC0037); Dr Lulu P. Shi; Prof Ekaterina Hertog; Prof Victoria Nash (TEC0039); 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 (TEC0048)
269 Which? (TEC0045) para 14
270 Horizon Digital Economy Institute, University of Nottingham (TEC0046)

98. We note specifically that aspects of the 2018 Code intersect with the remit of the ICO, such as data protection measures, secure data storage and secure communications. Indeed, as the Government argued when bringing forward the Data Protection Act 2018, "strong cyber security and data protection go hand in hand".[271] Cybersecurity is a safeguard for data processing: UK GDPR requires organisations to process personal data securely, under which the ICO's aims and outcomes include protecting personal data from cyberattacks and security monitoring.[272] Similarly, the NCSC lists privacy and data protection amongst its risk management principles for cybersecurity.[273] Practically speaking, regulatory co-ordination on product security and data protection could be achieved by the OPSS working with the ICO, either bilaterally or as part of the ICO's work within the Digital Regulation Co-operation Forum, which already brings together the ICO, Ofcom, the Competition and Markets Authority (CMA) and Financial Conduct Authority (FCA) to ensure a greater level of co-ordination in regulating online platforms and digital services.

99. Many submissions also called for greater assurance, certification and/or labelling for connected products. Technology assurance refers to assessments and statements of confidence in a product or system that help consumers make informed choices about the risks of using it (particularly in contrast to alternatives).[274] Certification (a formal attestation of meeting specific standards or requirements) and labelling (a physical identifier of certification displayed on a product or packaging) are methods of demonstrating that assurance has been given. Academic and industry contributions, including from Google, advocated for physical labelling (such as for privacy, data safety, security quality, and so on), citing benefits regarding incentivising security and privacy by design, informing consumer choice and reinforcing the importance of security in purchasing decisions.[275] However, REPHRAIN, the UKRI-funded National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online, warned that if done incorrectly labelling could have adverse effects or backfire such as by providing assurance for products that hadn't been sufficiently tested, inadequately presenting complex information and/or presenting levels of security as a static, rather than potentially quickly outdated, characteristic.[276] techUK similarly described a physical labelling regime as "impractical" and suggested it would not lead to greater consumer awareness.[277]

100. A range of academic and industry submissions called for some broader type of certification scheme.[278] NCC Group has advocated that manufacturers' compliance should be technically validated by independent third parties, in line with best practice for

271 Department for Digital, Culture, Media & Sport, Data Protection Act 2018 Factsheet - Overview, 25 May 2018
272 Information Commissioner's Office, 'Security outcomes', accessed 15 June 2023
273 National Cyber Security Centre, 'Risk management guidance', accessed 15 June 2023
274 National Cyber Security Centre, *White paper: The future of NCSC Technology Assurance* (24 September 2021)
275 Qq338, 348–51, 360; The University of Gloucestershire (TEC0020); REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); Horizon Digital Economy Institute, University of Nottingham (TEC0046)
276 REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043)
277 techUK (TEC0049)
278 Q103; Dr Efpraxia Zamani (TEC0011) para 6.2; Dr Ana Canhoto; Professor Ashley Braganza; Dr Asieh Tabaghdehi (TEC0018) para 3.3; NCC Group (TEC0024); REPHRAIN - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043); Horizon Digital Economy Institute, University of Nottingham (TEC0046) paras 18, 25; 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 (TEC0048); techUK (TEC0049); Age Check Certification Services Limited (TEC0059)

other sectors.[279] As Matt Lewis noted:

> […] there might still be a broad assumption that where legislation [and] regulation dictates certain requirements, those will actually get enacted. What might be missing is some sort of mandated independent third-party validation of security products systems, because that is when you get the evidential piece about where maybe the developer or manufacturer did make assumptions.[280]

Indeed, the Government has previously proactively administered a modest grant-making programme that supported product assurance schemes. The three successful bids were the Internet of Toys Assurance Scheme (combining the 2018 Code of Practice with the Age-Appropriate Design Code), Smart TV Cyber Assurance, a platform that detects vulnerabilities in smart TVs, and IASME IoT Security Assured, a self-assessment scheme for small and medium-sized enterprises (SMEs) to check compliance with the 2018 Code.[281] However, Age Check Certification Services Ltd, the operator of the Internet of Toys Scheme, told us that the programme was "a little ahead of its time" as "it quickly became clear that suppliers would not voluntarily incur the expense of certification until it was legally required" but nonetheless "the scheme stands ready for that day".[282]

101. **The introduction of the product security regime, which codifies three of the original thirteen guidelines set out in the Government's internationally recognised 2018 Code of Practice for Consumer IoT Security, is an important first step in improving cybersecurity for connected devices. However, the remaining ten guidelines retain considerable support among stakeholders.** ***We recommend that the Office for Product Safety and Standards (OPSS), as the national regulator, should produce an implementation plan so policymakers can measure the impact of the product security regime. The OPSS should continue to promote the guidelines not included in the Product Security and Telecommunications Infrastructure Act 2022 and the Government should commit to codifying these remaining guidelines in phases as the regime matures and industry adapts, in order to stay ahead of emerging cyber threats.***

102. **As the guidelines set out in the 2018 Code of Practice for Consumer IoT Security imply, cybersecurity and data protection are mutually reinforcing. Without cybersecurity, data cannot be meaningfully protected, while data protection can manage the risk and impact of cyberattack.** ***The Information Commissioner's Office, either bilaterally or through the Digital Regulation Co-operation Forum, which helps co-ordinate regulation of digital platforms and services, should work with the Office for Product Safety and Standards as it promotes the guidelines pertaining to data protection and data security in the 2018 Code of Practice.***

Cybersecurity for businesses

103. The NCSC has identified a lack of accepted sources of reliable assurance across the range of customers it serves and for the types of technologies available to them. Most notably, its White Paper on technology assurance illustrates that both large/multinational

279 Q103 [Matt Lewis]; NCC Group (TEC0024)
280 Q103 [Matt Lewis]
281 Department for Digital, Culture, Media & Sport, 'Grant Programme for Consumer IoT Assurance Schemes 2020/21', 14 June 2021; see also techUK (TEC0049); Age Check Certification Services Limited (TEC0059)
282 Age Check Certification Services Limited (TEC0059)

businesses and SMEs lack official means of assurance for off-the-shelf products and bespoke technologies used in enterprise settings, including operational technology and industrial control systems.[283] Legacy operational technology can pose a particular problem, as systems are designed to remain in use for decades and therefore may combine or overlay components that were never designed to be incorporated into smart systems or rely on software solutions that are less secure or are no longer supported with security updates.[284] Moreover, there are billions of these devices currently in operation.[285] However, despite the proactive work in addressing these gaps—such as the work by the Government and NCSC to develop device security principles for enterprise devices (albeit "to be tested and challenged by industry partners")[286]—NCC Group argues that "this remains voluntary, meaning manufacturers can easily ignore the principles without any real consequence".[287]

Cybersecurity in networks

104. Returning to the concept of the "stack" of components that comprise connected tech (see paragraph 6), the emphasis of the product security regime is to improve security at the device layers (predominantly through the device's software). However, there are several problems with this approach in lieu of a comprehensive effort to secure the entire stack. As such, an attacker may be able to compromise the connected system simply by exploiting attack vectors elsewhere in the stack. Other vulnerable layers may include apps, app stores, open networks and the wireless spectrum, servers and cloud computing environments.

105. This poses several issues, First, an attacker can simply bypass a secured device and access desired information as it is transmitted to other parts of the system. As Matt Lewis illustrated:

> A good example would be CCTV cameras and IoT cameras. You could make a really secure product that does that really well, and enforces all its security functions, but it might be transmitting the video feeds up to a cloud server, which is completely open. You don't necessarily have to compromise the device to get access to the information. You might be able to compromise another connected aspect of that technical ecosystem.[288]

Second, an insecure network, server and so on may be used as a vector to then compromise the device itself. Matt Lewis continued:

> For example, a lot of connected devices will talk out to the internet, to remote servers. There are a number of scenarios that could occur whereby an attacker may compromise the server that all of those devices communicate with, and then use that as a vector back into compromising a device. With typical phishing in the home network, if you get phished while connected to your home wi-fi network, suddenly the attacker has more privileged access to all the other devices on that network and can try an intrusion via that phishing attempt.[289]

283 National Cyber Security Centre, *White paper: The current state of technology assurance* (24 September 2021)
284 NCC Group (TEC0024)
285 Palo Alto Networks, *Governments Must Promote Network-Level IoT Security at Scale* (December 2021), p 6
286 Department for Digital, Culture, Media and Sport (TEC0054) para 18
287 NCC Group (TEC0024)
288 Q94
289 Q107

Third, relying on device-level security can have limitations. Palo Alto Networks has noted that it may be impossible to embed security in connected devices that lack the in-built storage and processing power (such as thermostats, smart lighting hardware and smart blinds), and that the heterogenous nature of connected devices makes a uniform built-in standard almost impossible.[290] As noted in the previous section, the billions of legacy devices also remain a challenge.[291] As a result, these easier-compromised devices may then be used to compromise other devices connected via an untrusted network. This issue is particularly relevant as working from home becomes more common, as employees connect otherwise-secured corporate-issued devices like laptops to untrusted home networks.[292]

106. Palo Alto Networks argues that device-level measures should be complemented by network-level security, cloud security solutions and machine learning. It cites three main benefits:

- Visibility and identification of devices, to help understand the system's attack surface and interdependencies in real time;
- Continuous device monitoring for anomalous traffic and threats (as the fixed functionality of connected devices often makes them predictable) to notify users of abnormal behaviours; and
- Security policy enforcement to react to anomalous behaviour in real time, automatically and at scale, such as by delivering risk reduction recommendations, segmenting networks and quarantining devices.[293]

107. The Government has taken limited steps to address other areas of vulnerability. In December 2022, the Government published a Code of Practice for app store operators, platform developers and app developers, which establishes eight principles for baseline requirements in security and privacy.[294] However, the Code remains voluntary and the Government intends to undergo several evidence-gathering steps from this year onwards.[295] Moreover, unlicensed wireless spectrum (such as open Wi-Fi networks), which remains unregulated despite underpinning the operation of a significant proportion of devices and sensors, has not yet received policy consideration.[296]

108. **Improving cybersecurity of consumer connected devices is an important and positive step, but the proliferation of connected tech in enterprise settings and the gap in the regime regarding network, storage and cloud security still present likely attack vectors that will continue to allow devices to be compromised. *The Government should close the gaps for both consumer and enterprise connected tech in the product security regime by requiring that providers adopt network-level, storage and cloud-based security to the same standards as it requires for connected devices.***

290 Palo Alto Networks, *Governments Must Promote Network-Level IoT Security at Scale* (December 2021), pp 5–6
291 Ibid., p 6
292 Ibid., pp 4–5
293 Ibid., pp 7–8
294 Department for Digital, Culture, Media & Sport, *Code of practice for app store operators and app developers* (9 December 2022)
295 Ibid.
296 NCC Group (TEC0024)

Cyber skills and workforce shortages

Skills in the wider economy

109. Connected tech still requires human intervention to undertake cyber hygiene measures. This human intervention therefore necessitates a level of digital literacy and skills to ensure that this does not compromise otherwise secure devices and networks. Despite this, there are significant and ongoing shortages of employees with the requisite technical and core professional skills within the cyber sector and the necessary cyber skills in the wider economy.

110. Government-commissioned research has found that 50 percent of all private sector businesses and 61 percent of charities report a lack of confidence in performing a range of basic cybersecurity tasks or functions, such as setting up firewalls, storing and transferring personal data securely and detecting and removing malware.[297] The proportion reporting a basic cyber skills gap is lower for large businesses (22 percent) and charities with incomes of £500,000 or more (36 percent); however, all businesses and charities trail public sector organisations in this regard by a significant margin, with only 10% of public sector organisations reporting a basic skills gap.[298] In terms of advanced technical skills, undertaken by dedicated cyber leads, such as forensic analysis, threat intelligence, interpreting malicious code and user monitoring, a third of businesses (33 percent) and a quarter of charities (26 percent) reported gaps in these areas.[299]

Skills in the cyber sector

111. For cyber sector firms themselves, research has found that almost half (47 percent) have faced problems with technical cyber security skills gaps, such as digital forensics, cybersecurity research and threat assessment, either among existing staff and/or job applicants.[300] Furthermore, a significant proportion of firms (31 percent) in the sector have experienced a skills gap in core professional (i.e. "soft") skills, such as communication, leadership and management skills, in either existing staff and/or job applicants; these skills are necessary for broader business functions including team working, awareness, training and culture change roles, and sales and client liaison functions.[301]

112. The sector is also experiencing a general workforce shortage for cyber professionals. This can be best illustrated by the cybersecurity workforce gap, which estimates the shortfall in individuals working in the profession relative to the demand for individuals, taking into account the growth in jobs relative to the current workforce and the net supply of professionals based on the number of individuals entering and leaving the field.[302] The Government has estimated, based on qualitative and quantitative research undertaken by Ipsos, that the workforce gap in the cybersecurity workforce for 2022 was approximately 14,100 per year, up from the previous year's estimate of approximately 10,000 by over 40 percent.[303] Written evidence from (ISC)², the largest international membership association

297 Department for Digital, Culture, Media & Sport, *Cyber security skills in the UK labour market 2022*, 3 May 2022, pp 23–5
298 Ibid., p 25
299 Ibid., pp 25–8
300 Ibid., pp 29–30
301 Ibid., pp 31–3
302 Department for Digital, Culture, Media & Sport, *Cyber security skills in the UK labour market 2022* (3 May 2022); (ISC)², *(ISC)2 Cybersecurity Workforce Study 2022*, accessed 3 May 2023
303 Q378 [Julia Lopez]; see also Department for Digital, Culture, Media & Sport, *Cyber security skills in the UK labour market 2022* (3 May 2022)

for cybersecurity professionals, however, put the workforce gap at approximately 56,800, up from the previous year's estimate of 33,000 by over 73 percent, based on research from its 2022 Cybersecurity Workforce Study.[304]

113. Both government and industry studies illustrate that despite proactive interventions, the workforce gap has continued to widen. Indeed, in the context of growing adoption of connected tech, the new product security regime and the increased demand in adjacent fields like data, software development, cloud computing and artificial intelligence, it is likely that the gap will continue to grow.[305] However, these figures should also be understood in the context of a global workforce gap.[306] (ISC)²'s 2022 Cybersecurity Workforce Study estimates that the global workforce gap stands at over 3.4 million, up over 26 percent year-on-year, underpinned by a 410,000 gap in the US alone (based on business surveys and studies by the US Bureau of Labor Statistics and the US Census).[307]

114. Both Government and industry have taken steps to address the cyber skills gap. The Minister listed a range of government interventions targeting both children and adults.[308] In schools, the Government has rolled out a free interactive learning platform called Cyber Explorers to teach essential digital skills and concepts to young secondary school pupils.[309] The Department for Education (DfE) has also recently announced a new T-Level in cybersecurity and will host three T-Level events, in London, Birmingham and Manchester, throughout the year in partnership with the UK Cyber Security Council (UK CSC).[310] For adult learners with a low level of digital skills, learners are able to access essential digital skills qualifications for free through the statutory digital entitlement administered by the DfE.[311] Through the NCSC, the Government has backed a technical standards certification scheme that recognise minimum levels of security within supply chains called Cyber Essentials.[312] The NCSC, in partnership with consulting and industry partners like NCC Group and others, manages the CyberFirst programme, a series of activities like summer schools, a higher education bursary scheme, girls' only competitions, a degree apprenticeship scheme and more.[313] Industry is similarly taking action: (ISC)² has pledged a 100,000 free courses and exams to individuals in the UK to support them with certification, education and skills and career development for entry- and junior-level cyber roles.[314]

115. The persistence of the skills gap, however, indicates that further work is needed. One area where more work can be done is in reducing disparities based on gender and race and ethnicity in the sector. Research shows that globally, the cyber labour market has a particularly drastic gender divide: Microsoft has argued that in the 23 countries, including the UK,[315] where it has launched national skilling campaigns, only 17 percent of

304 (ISC)2 (TEC0066); (ISC)², *(ISC)2 Cybersecurity Workforce Study 2022*, accessed 3 May 2023; see also (ISC)², *(ISC)2 Cybersecurity Workforce Study 2021*, accessed 3 May 2023
305 (ISC)2 (TEC0066)
306 Q110
307 (ISC)², *(ISC)2 Cybersecurity Workforce Study 2022*, accessed 5 May 2023
308 Q378
309 Q378; see also Department for Digital, Culture, Media & Sport, 'Cyber Explorers', 23 February 2022
310 UK Cyber Security Council, 'Why you should be paying attention to T-Levels', 20 April 2023
311 Q378; see also Department for Education, 'Free qualifications for adults with low digital skills', 31 March 2022
312 Department for Digital, Culture, Media and Sport (TEC0054) para 24
313 Q98, 110; National Cyber Security Centre, 'CyberFirst overview', accessed 9 May 2023
314 (ISC)2 (TEC0066)
315 Microsoft, 'Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries', 23 March 2023

the workforce is female.[316] (ISC)²'s workforce study, which breaks down the gender divide by age groups, shows only limited progress among younger cohorts, with women still only comprising 30 percent of under 30s and 24 percent of 30–38 year olds working in the sector (albeit up from 14 percent of over 60s, 12 percent of 50–59s and 13 percent of 39–49s).[317] (ISC)² also ranked the UK as among the least gender diverse countries for cyber. The gender disparity is also most stark in sectors like healthcare, insurance, financial services and consulting, in comparison to retail, entertainment and engineering.[318] Additionally, (ISC)² found that there is a global disparity based on both gender and race and ethnicity at executive and managerial roles compared to entry-level roles.[319] Microsoft has also highlighted the need for more teachers able to teach cybersecurity learners.[320] Similarly, the World Economic Forum has called on industry to the industry improve hiring practices in order to widen the talent pool, citing a need to "promote clear requirements for roles, including job qualities and skills" and for flexibility in hiring "that perhaps focuses on capabilities over certifications".[321] Conversely, no evidence we received discussed improving retention and providing broader, core professional skills, on-the-job retraining and other support for existing cybersecurity professionals, which may address the wider skills gap within the cybersecurity sector. However, the World Economic Forum has called on organisations to better manage underlying factors like pressure and burnout to improve retention rates, such as by offering flexible working arrangements and employee wellbeing solutions.[322]

116. **We are concerned about the ongoing skills shortage, as recognised in both the Government and industry's regular reporting on cybersecurity skills in the labour market, and believe that the shortage will be exacerbated further as the product safety regime comes into force. We support industry's calls for the Government to do more to address this issue.** ***The Government should also take steps to support the availability of free courses across the country, encourage more professionals to become cybersecurity educators, improve the provision of core professional skills among the existing workforce and incentivise industry to improve hiring practices and retention rates.***

117. **We are particularly concerned that, despite the shortage of cyber skills in the UK, there are stubborn and significant disparities in the cyber workforce based on gender and race and ethnicity.** ***The Government should reflect on the significant disparities in gender and race/ethnicity in the cyber workforce and take steps to improve these divides, such as by introducing additional schemes and funding to widen the talent pool, improving the culture of and attitudes to the cyber profession both in education and work, and considering how to provide professional support for people during their career.***

316 These countries are: Brazil, Poland, Denmark, Germany, Sweden, Switzerland, Belgium, Japan, Mexico, Norway, Colombia, France, Israel, New Zealand, the UK, Canada, Australia, India, Ireland, Romania, South Africa, Italy (ranked in terms of gender disparity from LinkedIn data) and South Korea (no data available). The scheme already operates in the US.

317 (ISC)², *(ISC)2 Cybersecurity Workforce Study 2022*, accessed 5 May 2023

318 Ibid.

319 Ibid.

320 Microsoft, 'Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries', 23 March 2023

321 World Economic Forum, 'The cybersecurity skills gap is a real threat — here's how to address it', 2 May 2023

322 Ibid.

Government capacity

118. The UK's strategic and policy responsibilities for responding to cyber threats and exercising offensive cyber power are dispersed across Government, including the Cabinet Office (responsible for the Government's response to cyber threats and fulfilling cyber power), Ministry of Defence, Foreign, Commonwealth and Development Office, the Home Office (collectively responsible for detecting and disrupting adversaries and countering cybercrime) and, since the February machinery of government changes, the Department for Science, Innovation and Technology[323] (the cyber economy, cybersecurity in the wider economy and developing innovation and skills).[324] All ministers are charged with providing oversight of the cyber security of their departments and implementation of appropriate mitigations.[325] However, a 2018 Report by the Joint Committee on the National Security Strategy (JCNSS) described the arrangements of ministerial responsibility as "complex", with "day-to-day oversight of cross-government efforts […], in reality, led by officials, with Ministers only occasionally 'checking in'".[326] In its response, the Government described the arrangement as "the most effective way of achieving our vision of cyber security as a core" with ministerial responsibilities "clearly defined" and "necessarily distributed across departments".[327] During our inquiry, evidence we heard would suggest that little has changed, with the attitude within Whitehall being described as "too rear-view mirror-focused, as opposed to forward focused"[328] due to "a lack of interest at the political level".[329]

119. The UK also has several agencies, bodies and networks that deliver analytical and operational cyber capability, including offensive cyber power. These include:

- The NCSC, formed in 2016 as part of GCHQ to be the UK's national authority on the cybersecurity environment;
- The National Cyber Force (NCF), responsible for the UK's offensive cyber capability, jointly staffed by intelligence and defence personnel;
- The national cybercrime network, co-ordinated by the National Crime Agency's National Cyber Crime Unit, connecting Regional and Local Cyber Crime Units; and
- The UK Cyber Security Council, a government-mandated self-regulatory body for the cyber security profession launched by DCMS in 2021.

However, there have been longstanding concerns that the Government is not able to meet the demand for cybersecurity services in particular. The 2018 JCNSS Report, for example, concluded that "we […] have concerns about the capacity of the NCSC to meet growing

323 Previously these responsibilities were discharged by the Department for Digital, Culture, Media and Sport.
324 HM Government, *National Cyber Strategy 2022* (15 December 2021)
325 Ibid.
326 Joint Committee on the National Security Strategy, Third Report of Session 2017–19, *Cyber Security of the UK's Critical National Infrastructure*, HC 1708, para 79
327 Joint Committee on the National Security Strategy, Third Special Report of Session 2017–19, *Cyber Security of the UK's Critical National Infrastructure: Government Response to the Committee's Third Report of Session 2017–19*, HC 2003, p 11
328 Q103
329 Q105 [Damian Green]

demand for its services and expertise" due to limited resources and access to experts.[330] Industry witnesses highlighted the need for further capacity-building within the NCSC itself, both to help improve resilience within the wider economy as well as in the context of the global workforce shortage.[331]

120. **The creation of the Department for Science, Innovation and Technology is an opportunity to ensure a comprehensive, joined up approach to cyber policy.** ***We recommend that responsibilities for cyber policy is co-ordinated by the dedicated Department for Science, Innovation and Technology and that government ensures collaboration between the Department and other cyber-focused teams distributed across Whitehall. Ministers in the Department for Science, Innovation and Technology should be ultimately responsible and accountable for developing and delivering cyber policy except for national security measures.***

121. **As the prevalence of connected technology grows, so too will the demand for the National Cyber Security Centre's services.** ***The Government should ensure that the National Cyber Security Centre has the capacity to meet demands for its services. It should explicitly consider and address capacity issues as part of its regular reporting on cybersecurity skills in the UK.***

330 Joint Committee on the National Security Strategy, Third Special Report of Session 2017–19, *Cyber Security of the UK's Critical National Infrastructure: Government Response to the Committee's Third Report of Session 2017–19*, HC 2003, p 11

331 Qq109–110

3 Technology-facilitated abuse

122. Technology-facilitated abuse, known as "tech abuse", describes a form of domestic abuse where perpetrators use technology, including connected devices and social media, to abuse victims and survivors.[332] The Domestic Abuse Act 2021 provides a new statutory definition of domestic abuse, which involves any single incident or course of conduct where one person's behaviour towards another is abusive, where the people involved are aged 16 or over and are, or have been, personally connected to each.[333] Children are considered victims of abuse if they see, hear or experience (the effects of) abuse and are related to or the responsibility of either person.[334] Tech abuse is a significant related issue because technology, and particularly connected technology, can broaden and exacerbate patterns of abuse and the reach of perpetrators, as perpetrators no longer need to be physically co-present with victims and survivors in order to inflict abuse.[335]

123. Tech abuse is becoming increasingly common.[336] According to Refuge, the largest specialist provider of gender-based violence services in the UK, more than a quarter of women aged between 16 and 74 in England and Wales experience domestic abuse at some point in their lives and, of the women and children it supported in 2020–21, 59 percent experienced abuse involving technology.[337] Dr Leonie Tanczer, Lecturer in International Security and Emerging Technologies and Principal Investigator of the Gender and IoT (G-IoT) Project at University College London (UCL), provided even starker figures, noting that some support organisations "say they have figures between 75 percent, 85 percent and […] 100 percent", with the Suzy Lamplugh Trust, a charity aiming to reduce the risk and prevalence of stalking and harassment, having said that "100 percent of their cases have a cyber element".[338]

Patterns of tech abuse

How devices are used

124. There are several ways that connected devices are exploited for or exacerbate behaviours and patterns of domestic abuse:

- Perpetrators are often the ones who purchase, set up and manage connected devices or force victims and survivors to diverge passwords to their accounts, establishing coercion and control.[339] Perpetrators may then use this access to further install intrusive or surveillance apps and software, called "spyware" or "stalkerware".[340] Dr Tanczer argued that the gender dimension of decisions relating to household tech was an exacerbating factor;[341] market research carried

332 Home Office, *Domestic Abuse: statutory guidance* (13 April 2023)
333 Domestic Abuse Act 2021, sections 1–2
334 Domestic Abuse Act 2021, section 3
335 Q3
336 Qq3, 96, 302, 383; Refuge (TEC0012); Dr Leonie Tanczer (TEC0021)
337 Refuge (TEC0012)
338 Qq4–5, 36
339 Qq37–8; Refuge (TEC0012) paras 9, 23; Dr Leonie Tanczer (TEC0021); see also Elizabeth Yardley, "*Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework*," Violence Against Women, vol 27 (10), 2020, pp 1479–1498
340 Q37
341 Q38

out by Refuge and Avast found that 27 percent of UK women stated that admin access for connected devices has not been shared equally or with transparency in their household and 18% of women said they have no control over the Wi-Fi settings in their home, but that their partner or family member does.[342]

- Perpetrators can also use connected devices to overtly coerce and control victims and survivors, even when they are not physically present.[343] Victims and survivors may overestimate the capabilities of devices, which allows perpetrators "to persuade or mislead their victim/survivor that their devices can perform certain activities, such as record video or audio, or access their personal device, when they cannot".[344]

- Perpetrators can use connected devices to covertly "monitor survivors' movements and locations, to listen in on conversations, collect recordings and intimate images for blackmail".[345] Often, connected devices may look innocuous, be easily disguised as normal devices or may be (pre)loaded with spyware or stalkerware.[346] Victims and survivors may also underestimate the capabilities of connected devices they see, use and interact with.[347] Features with remote access and/or geolocation functions may enable perpetrators to continue to monitor, communicate and exert coercion and control after survivors have fled.[348]

- Perpetrators can use connected devices to retaliate against victims and survivors. This can include using remote and automated functionalities to manipulate devices or the material environment of a victim/survivor to "gaslight" and cause fear, confusion and distress to inflict emotional and psychological harm.[349] As noted above, devices may also be used to collect recordings and images for blackmail purposes, including from strangers or acquaintances.[350] Connected tech may also compromise physical safety by disclosing their location even after they have fled;[351] as Dr Tanczer noted:

  > People now need to think, "If I go into a refuge, is my smartwatch still connected with my device?" Interestingly, people have found that women are often detected in the refuge through their Netflix account because they forget that they are still connected when they log in at the refuge. It is these things that women are not thinking of, and of course they aren't.[352]

125. Tech abuse may also have indirect implications caused by the data collected by connected devices while a victim/survivor is being coerced or controlled by a perpetrator.

342 Refuge (TEC0012) para 9
343 Elizabeth Yardley, "*Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework*," Violence Against Women, vol 27 (10), 2020, pp 1479–1498; see also "*How smart devices are exploited for domestic abuse*", BBC News, 18 October 2020
344 Dr Leonie Tanczer (TEC0021)
345 Refuge (TEC0012) para 6
346 Q3; Refuge (TEC0012) para 14; see also *Technology and domestic abuse*, Rapid Response, Parliamentary Office of Science and Technology, 13 November 2020
347 Q3
348 Refuge (TEC0012) para 9; Dr Leonie Tanczer (TEC0021)
349 Q3; Refuge (TEC0012) paras 6–7, Dr Leonie Tanczer (TEC0021); see also *Technology and domestic abuse*, Rapid Response, Parliamentary Office of Science and Technology, 13 November 2020
350 Q37; Refuge (TEC0012) para 6
351 Qq37–39; Refuge (TEC0012) paras 7–8
352 Q39

The data collected by connected devices, and the data records and profiles that are subsequently created, may therefore present an inaccurate representation of the victim/survivor.[353] This may then have implications for accessing services like banking and insurance as risk patterns and behaviours, financial credit ratings and health profiles may reflect these inaccurate representations.[354]

Types of devices used

126. These broad patterns mean that a variety of devices may be exploited by perpetrators. Smart home security systems, smartphones and tablets, wearables and other smart home apps and devices like connected toys, baby monitors, cameras and smart speakers have been cited among the most common devices used to monitor, harass, coerce and control victims and survivors.[355] Smart appliances are often used for covert monitoring due to the relative difficulty to distinguish from normal appliances.[356] As Jessica Eagleton, Refuge's Policy and Public Affairs Manager, told the Product Security and Telecommunications Infrastructure Bill Committee:

> Some of the most common devices we see reported to us include your smart home hubs, smart voice assistants, smart TVs, plugs, light switches and fitness trackers. […]
>
> Perpetrators quite often set up a host of different devices in the home. Recently, we supported a woman whose former partner had bought a whole host of devices, including smart cameras, a smart doorbell, a smart thermostat—all those kinds of things. She and her child felt like they were constantly being monitored; they talked about how exhausted they were by that constant surveillance.[357]

Refuge also notes that "devices gifted to children are used to continue exerting control post-separation and can enable the perpetrator to access audio-visual information and to track the address of the new location the survivor has fled to".[358] Alarmingly, Refuge also asserts that it is "aware of devices on the market that are designed and promoted for the specific purpose of stalking and harassment, masquerading as home tech or home security products" and are openly advertised and sold online.[359]

Devices used by victims and survivors

127. Several contributors also noted that connected devices could have benefits in tackling tech abuse. Dr Tanczer noted that "IoT-connected devices have a lot of benefits for victims and survivors, police services, support services, and so on".[360] Amazon's Leila Rouhi discussed examples of the company's work with support services:

353 Dr Leonie Tanczer (TEC0021)
354 Q3; Dr Leonie Tanczer (TEC0021); see also Q351
355 Q36; *Technology and domestic abuse*, Rapid Response, Parliamentary Office of Science and Technology, 13 November 2020
356 Q3
357 Product Security and Telecommunications Infrastructure Bill, Q75
358 Refuge (TEC0012) para 8
359 Refuge (TEC0012) paras 7, 14, 29
360 Q3

> We do work with domestic violence organisations, including work to support their missions when it comes to survivors. We have heard from them that connected cameras are one of the most requested types of devices for survivors, oftentimes when they are leaving a shelter and trying to re-establish their lives. Having the peace of mind of knowing who is in and around their home if they have a protection order, having that awareness if the person that they are seeking protection from is on the property, that is an incredibly powerful tool for survivors.[361]

The Minister similarly echoed these sentiments, noting that "sometimes domestic abuse victims actually welcome connected products on the basis that they can also monitor their homes and make sure they are aware of any security breaches".[362]

Tackling tech abuse

Criminal justice response

128. Compounding the issue further is that the criminal justice response to tech abuse is lacking, even in comparison to other forms of domestic abuse. It should be noted that the Government, for example, has included tech abuse ("technology-facilitated abuse") in its statutory guidance to raise awareness of and inform the response to domestic abuse, issued under the Domestic Abuse Act 2021.[363] The guidance is aimed at organisations working with victims and survivors, perpetrators and commissioning services, including the police, local authorities, and the NHS, as well as employers and financial institutions.[364] However, contributors argued that while the Government has taken some positive steps, there are still further actions needed. Refuge, for example, has argued that:

> Too often, the onus is placed on survivors to change their behaviour, with police officers recommending survivors come offline, rather than focusing on pursuing perpetrators. Officers frequently lack an understanding of the nature and dynamics of domestic abuse, and the dangers and multiple forms of tech abuse.[365]

Dr Tanczer further explained why it was impractical to simply expect victims and survivors to "go offline":

> The problem is—and we hear this repeatedly—where police say to just go offline. You cannot go offline. My life is dependent on being online. Whether you have a public profile, or it is your job or public services, you cannot expect that anyone does this nowadays. We need to find a solution where people can remain online and have a presence online, which is necessary for their livelihood. That is one issue. Police need to take this seriously and not consider this as a less horrible thing.[366]

361 Q351
362 Q384 [Julia Lopez]
363 Home Office, *Domestic Abuse: statutory guidance* (13 April 2023)
364 Ibid.
365 Refuge (TEC0012) para 20
366 Q40

129. These perspectives were supported by the Information Commissioner, who similarly questioned whether law enforcement had the necessary skills to address tech abuse:

> I do think that there will be cases in which police forces are ill-equipped to help a victim navigate the technical settings that they need to do to reclaim their autonomy and their control over these devices, for example. We know that beat cops may not be hugely technically savvy, and so while they can press charges against somebody who continues to harass and intimidate, they may not be well placed to assist a victim to engage with the provider, to reset the security settings and the like.[367]

130. techUK's Deputy CEO, Antony Walker, similarly advocated for a comprehensive response to tech abuse that involved upskilling law enforcement and improving support for victims and survivors:

> These are extraordinarily complex situations about human interactions. In some of these areas the solutions may not be with the tech. The solutions need to be about how we come in to support people in these situations, how law enforcement works in these situations and how law enforcement better understand technology in these situations. Sometimes you do not always have to come at it by layering on another bit of regulation to tech. Sometimes it is about recognising that this is a societal problem and working out how to address it.[368]

131. **The Government must make tackling technology-facilitated abuse, or "tech abuse", a priority. There is little evidence to suggest that our law enforcement and criminal justice system has been equipped to deal with the problems caused by tech abuse now, let alone as connected devices become even more prevalent in future. While there is no "silver bullet" for dealing with tech abuse, the Government can do more to tackle it.**

132. ***The Government's response to tech abuse should involve upskilling law enforcement to improve the criminal justice response and increasing law enforcement's and victims' and survivors' awareness of specialist services tackling violence against women and girls. The Government should also reflect on how official crime data on tech abuse can be improved to expand the evidence base for specialists, academics and policymakers in order to develop a more comprehensive, co-ordinated response.***

Public awareness

133. As with other forms of product security, digital literacy is an integral part of the response to empower users.[369] Professor George Loukas, from the University of Greenwich, for example argued that "if there is a significant disparity between the digital literacy of the persons involved, you might have someone who is exploiting access to the app while the other person does not know that the app is collecting the data".[370] However, public awareness of tech abuse is low: Refuge has found that "nearly half (48 percent) of women are unable to name a home device they believed could be vulnerable to abuse—increasing to 60 percent for those aged over 55" and that "two-thirds of women surveyed (66 percent)

367 Q303
368 Q48
369 Refuge (TEC0012) para 17
370 Q96

did not know where to get information to help secure devices in their home if they felt that had been compromised by an abuser, rising to 79 percent for those aged 45 and over".[371] Professor Loukas also noted that tech companies' own support staff often do not know how to respond to these types of reports.[372]

134. Several contributors proposed ways of increasing public awareness about tech abuse beyond broader steps to improve digital literacy. Dr Tanczer, for example, advocated the digital literacy work of the Australian Office of the eSafety Commissioner—who we took evidence from in our pre-legislative scrutiny of the Online Safety Bill[373]—which acts as "a centralised public body that provides information, help and support for the Australian public about online risks and harms".[374] From the industry perspective, Google's David Kleidermacher discussed the importance of better informing users of risks by including "notifications and visual indicators" and "things that we can do in mobile devices to alert the user that there may be something going on".[375] However, the seamless design and lack of visual display for most connected devices often means that this is hard to discern for most users.[376] Importantly, Refuge has urged that "caution should always be exercised regarding the inadvertent education of perpetrators on new ways to abuse".[377]

Industry response

135. Many contributors asserted that industry had a role to play in making devices safe and secure for all people. Google and Amazon, for their part, acknowledged that devices could be misused or abused and affirmed that tackling this had been a priority.[378] Amazon's Leila Rouhi told us that the company had "engaged in the United States with experts in domestic violence and tech abuse to understand the needs of these consumers and understand what types of features and choices we can build to enable these customers".[379] David Kleidermacher similarly highlighted that Google has introduced an "advanced protection programme, where people can opt into a high level of safety and privacy in their Google accounts" and "comprehensive programmes to counter what we call stock adware and spyware that can be abused".[380] Despite this, Refuge emphasised that "the response from technology companies to survivors of tech abuse can often be poor", both for individuals—noting that requests to help victims and survivors make changes to security settings or regain admin control of devices were often slow to process or refused outright—and at a systemic/design level.[381] It also noted that the framework for reporting security flaws contained a loophole whereby manufacturers do not have to take steps to fix these flaws before they are publicly disclosed to consumers, which could alert perpetrators to vulnerable devices.[382]

371 Refuge (TEC0012) para 17; see also Product Security and Telecommunications Infrastructure Bill, Qq69, 76
372 Q96
373 Oral evidence taken before the Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation on 14 December 2021, HC (2021–22) 620
374 Dr Leonie Tanczer (TEC0021)
375 Q350
376 Q97
377 Refuge (TEC0012) paras 17
378 Q350
379 Q350
380 Q350
381 Refuge (TEC0012) paras 12–4
382 Ibid., para 24

136. Several contributors also argued that issues with the industry response to tech abuse were a result of broader issues with the market. On the one hand, Dr Tanczer contended that the market power of Big Tech manufacturers like "Amazon, Apple and Microsoft" accrued by locking-in consumers to their device and software ecosystems allowed them to set the technical standards for the market or otherwise acquire disruptive start-ups, which undermines innovation (such as pro-privacy, data portability and interoperability, which might otherwise threaten the ecosystems' lock-in effects).383 Dr Tanczer recommended that Government could diversify the market by (continuing) funding start-ups, providing other financial incentives, setting common standards and investing in university research.384 On the other hand, David Kleidermacher argued that Big Tech firms were more able to invest in addressing the risks of tech abuse, and were therefore more able to innovate before the "long tail" of smaller manufacturers.385 Mr Kleidermacher instead advocated for more public-private partnerships to collectively create better technical standards and transparency across industry, particularly when protecting higher-risk populations, citing "the security ingredients label, accessibility requirements and responsible AI" as supportive examples.386

137. There have been some positive steps to build on. Multinational tech and industrial research corporation IBM has proposed what it describes as "five key design principles" to tackle tech abuse, set out in a November 2020 report. These principles are:

- Promoting diversity in design teams;
- Guaranteeing privacy and choice (e.g., making settings easier to understand);
- Combating gaslighting (e.g., by having local settings override remote settings);
- Strengthening security and data; and
- Making technology more intuitive.387

App-based bank Monzo has added a "Share With Us" function, which allows customers to disclose sensitive information discretely and safely, and the option to set up a code word in case they are concerned that their activity is being monitored.[388]

138. ***We want to see words from cross-sector stakeholders on tech abuse now leading to positive actions. The Office for Product Safety and Standards should, at the earliest opportunity, convene a "tech abuse working group" with stakeholders, bringing industry together with researchers, specialist support services and public services. This group should be more than just a talking shop, and draw on research to produce guidance and a code of practice that establishes best practice for manufacturers, vendors and law enforcement. The working group should report publicly through the OPSS on its progress at regular intervals.***

383 Qq42–44; Dr Leonie Tanczer (TEC0021)
384 Q43; Dr Leonie Tanczer (TEC0021)
385 Q351
386 Q351
387 IBM Academy of Technology, *Five Technology Design Principles to Combat Domestic Abuse* (November 2020)
388 *Technology and domestic abuse*, Rapid Response, Parliamentary Office of Science and Technology, 13 November 2020

Annex 1: Glossary of terms

Term	Definition	Synonyms and *examples*
Actuator	A component that controls or moves a device.	
Artificial intelligence	An autonomous system that generates outputs (e.g., content, predictions, recommendations and decisions) and improves performance based on data inputs to achieve goals set by its programmers.	AI Machine learning
Augmented reality	An interactive experience that combines or overlays computer-generated content over the real world.	AR
Cloud computing	Dispersed, remote computing services, such as data storage or processing, available over the internet and typically on-demand.	*Amazon Web Services (AWS)* *Google Cloud* *iCloud (Apple)* *Microsoft Azure*
Connected tech	An electronic device that can: operate remotely or autonomously; and connect to the internet, networks and/or other devices wirelessly.	Connected device Smart device Internet-connected device Consumer connectable device Internet of Things device
Connectivity protocols and standards	Rules that dictate how data is sent between and across devices, networks, servers, etc.	
Creative technology	Technology that enables the creative industries to produce new experiences, services, products and other forms of cultural activity.	CreaTech
Cyberattack	An intentional effort to compromise (steal, alter, disable, destroy, etc) data, applications or assets through unauthorised access to a digital device, computer system or network.	
Cyber hygiene	An evaluation of whether an individual or organisation takes regular, precautionary steps to mitigate against the risk and impact of cyberattack, like changing passwords, updating software and scanning for viruses.	
Cyber resilience	The ability for households and organisations to prepare for, respond to and recover from cyberattacks.	

Term	Definition	Synonyms and *examples*
Cybersecurity	The practice of protecting electronic information, digital devices, computer systems and networks from cyberattack.	
Data controller	A person or organisation that determines the purposes and means of the processing of personal data.	
Data processing	A range of activities, including collecting, recording, using, analysing, combining, disclosing or deleting data.	
Data protection	The process of protecting information from unauthorised access, theft, loss or corruption.	
Data subject	An identified or identifiable living individual to whom specific personal data relates.	
Digital twin	A simulation created from data gathered about a person, device or environment, which can then be used to run tests to learn how that subject might respond in hypothetical scenarios.	
Edge computing	Where data processing and analysis happens on data servers in close geographical proximity to devices in the network (in contrast to cloud computing).	
Firmware	Low-level programs that boot up and operate the device's hardware components.	
Gateway	A router or server that connects a multitude of other devices to the internet and aggregates, processes and analyses data and transmits commands to and from those devices at once.	
Generative AI	Artificial intelligence that generates images, text and other types of media in response to prompts.	*ChatGPT (and Bing Chat)* *DALL-E* *Midjourney*
Hardware	Physical components of a device.	*Actuators* *Microphones* *Processors* *Sensors*
Internet of Things (IoT)	Can be used either generally when referring to networks of connected devices, or more specifically to describe the point in time where there are more devices that are connected to the internet than people (estimated approx. 2015).	
Nearables	Devices that only work in close proximity to other devices.	

Term	Definition	Synonyms and *examples*
Operational Technology	Hardware and software that monitors, manages and controls an organisation's industrial operations. Often found in warehouses or outdoor areas like car parks.	OT
Personal data	Data that relates to an identified or identifiable individual.	
Processor	A component that responds to and executes instructions.	
Sensor	A component that detects events or changes in the device's surrounding environment.	
Shared virtual environment	Hypothetical iterations of the internet and/or computer systems that are represented as a single, immersive, holistic virtual world or platform where users can socialise, work, play, etc.	The metaverse *Horizon Worlds (Meta)* *ifland (SK Telecom)*
Smart city	An urban environment with networks of connected technology to collect data from citizens, other devices, buildings and assets. This is then used to manage assets, resources, public services, institutions and city planning and governance.	
Smart environment	Networks of devices in a specific physical location connected together to perform everyday tasks.	*Smart homes* *Smart cities* *Smart manufacturing* *Smart workplaces* *Smart schools*
Smart home	Connected devices within a building that can monitor and control attributes like lighting and climate.	Domotics Home automation
Smart meter	A device that records information such as energy and water usage in a home and enables two-way communication between a supplier and the device. Typically records data on consumption for billing purposes.	
Smart speaker	A loudspeaker that can connect to networks/devices and integrates a voice-activated virtual assistant.	*Amazon Echo, Amazon Echo Show* *Apple HomePod* *Google Nest, Google Home*
Software	Programs, instructions and data that run the device.	

Term	Definition	Synonyms and *examples*
Special category data	Types of personal data that are particularly sensitive. UK GDPR defines these as: data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); concerning health; concerning a person's sex life; and concerning a person's sexual orientation.	
Telemetry	Data from measurements taken *in situ* to monitor specific things, ranging from meteorological data taken by weather balloons (to create forecasts) to performance data from a device or its operator.	
Virtual assistant	A computer program that performs tasks based on voice commands or questions. Included in smartphones, smart speakers, computers, etc. Typically activated by a "hot word" that signals to the assistant that the subsequent command should be sent to the cloud for processing.	*Alexa (Amazon)* *Cortana (Microsoft)* *Google Assistant (Google)* *Siri (Apple)*
Virtual reality	A simulated, digitally-rendered experience that immerses the user in a virtual world.	VR
Wearables	Body-borne devices, such as smartwatches, smart glasses and fitness trackers. Often used for health purposes and include sensors like heartrate monitors, accelerometers, altimeters, thermometers, GPS, etc.	*Apple Watch* *Apple Vision Pro* *Fitbit* *Google Glass* *Meta/Oculus Quest)*

Annex 2: Visit to the Republic of Korea

MONDAY 23 MAY	
11:00	Intro meeting and visit pre-brief with Deputy Head of Mission (Chargé d'Affaires) Meeting will discuss political context in Korea, particularly following the recent Presidential elections, as well as the UK's objectives in Korea and the role of the Embassy in working to achieve these objectives.
12:00	Working lunch at local restaurant with BE Seoul officials.
14:00	Meeting with MPs, government officials and creative industry representatives Meeting with three MPs of National Assembly Standing Committee for Culture, Sport and Tourism, two government officials from Ministry of Culture, Sports and Tourism (MCST), five creative industry representatives and an academic from Korea Development Institute, a government think tank.
16:00	Meeting with senior members of SM Entertainment and tour of company Meeting with senior members of SM Entertainment to learn 1) the scope of their business, 2) their international collaboration and audience engagement programmes and 3) their plans related to use of digital technologies. This follows a 15-minute company tour.
TUESDAY 24 MAY	
09:00	Pre-brief with VisitBritain CEO Patricia Yates
09:35	Roundtable: Beyond London A roundtable discussion with experts from the South Korean outbound travel sector, alongside BE Seoul's Chargé d'Affaires, Nikesh Mehta, and Visit Britain CEO, Patricia Yates. Exam question: why do most South Korean visitors to the UK travel beyond London? What are the barriers that prevent them leaving London and how can we encourage them to explore the rest of the UK?
11:55	Traditional Temple Lunch with Korean Tourism Organisation and tour of temple Discussion on the operations of the Korean Tourism Organisation, and how the promote Korea as a destination for tourism.
13:00	Jogyesa Temple Tour
15:00	Working Holiday Event: Youth Mobility Scheme ROK Ministry of Foreign Affairs will lead this event highlighting the working holiday scheme between ROK and UK. Up to 50 young people who have been granted a visa to come to the UK for up to two years for the working holiday scheme will be in the audience. A former participant in the scheme will discuss their experience visiting Britain and then VisitBritain CEO will give 5 - 10 mins remarks welcoming them to the UK followed by questions.

16:00	Meeting with SK Telecoms (SKT) and tour of SKT T.um exhibit Meeting with SK Telecom to discuss 1) 5 & 6G, 2) broadband, 3) AI and digital infrastructure, and 4) up and coming tech and tech trends e.g., the metaverse. The meeting will be followed by a one-hour tour of their interactive tech-showcasing exhibit.
WEDNESDAY 24 MAY	
07:00	Tour of DMZ Joint Security Area
13:30	Working lunch with HMA Colin Crooks
15:30	Roundtable discussion with four creatives Roundtable discussion with four creatives to listen to their journey for global success, their insight of how K-style has won global attention and their views on how policy can support creative talents working internationally. This session will be facilitated by Fiona Bae, the author of an upcoming book, Make Break Remix: The Rise of K-style.
THURSDAY 26 MAY	
08:00	BCCK Breakfast Event British Chamber of Commerce Korea industry event on Korea's Entertainment Industry in 2022: Business Models, Success Stories and Future business Opportunities.
09:35	Intro meeting with the BCCK Executive Director Lucinda Walker
11:00	Meeting with National Assembly MPs [Digital Agenda] Discussion with National Assembly MPs from the Ministry of Science and ICT Committee, and other MPs with an interest on online safety. Agenda will cover 1) the metaverse 2) online safety and 3) protecting human rights online.
14:10	Meeting with Samsung Electronics Vice President Meeting with Samsung Electronics representatives to discuss 5&6G, ORAN, Semiconductors, Samsung's predictions/priorities for upcoming important tech trends, and Samsung's business interests in the UK.
14:40	Guided tour of Samsung Innovation Museum
17:50	Queen's Birthday Party
FRIDAY 27 MAY	
10:00	Meeting with KENAZ Studio and studio tour Meeting with Woojae Lee, CEO of KENAZ to learn 1) the scope of their business and 2) Korean webtoon business, followed by a 20 mins studio tour.
11:00	One-hour meeting with officials from Korea Creative Content Agency (KOCCA)
12:30	Meeting with the CEO of Ocon Studio and company tour Meeting with Ilho Kim, CEO of Ocon Studio to learn 1) the scope of their business, 2) their international collaboration and audience engagement programmes and 3) their plans related to use of VR/AR technologies. The meeting will be followed by a studio tour.

15:30	Meeting with National Assembly Representatives with an interest in China Discussion topic: Korean foreign policy navigating the US/China rivalry. Korean Parliamentarians will give presentations, followed by a discussion/ Q&A session.
17:30	Wash-up meeting with HMA and DHM

Conclusions and recommendations

Data and privacy

1. Data rights are an important tool for empowering data subjects and balancing data processing against users' rights and freedoms. However, there are many barriers to individuals being able to exercise these rights when using or interacting with connected tech, ranging from product design to digital literacy and resources. Users must be given clear information about, and a fair chance to understand, the basis on which their data is used, the implications for their digital rights, the benefits and risks, and how to consent, object and how to exercise these rights. (Paragraph 35)

2. *The Government should introduce appropriate measures to standardise privacy interfaces for connected devices as a first step, which will help users learn how to control connected devices in their homes and exercise data rights. Privacy interfaces should be appropriately accessible, intuitive and flexible enough so users of a reasonable level of digital literacy and privacy expectations can use them, without requiring them to go through complex dashboards with long lists of terms and conditions and settings. Interfaces should also provide information on how devices are connecting to other devices and networks, to provide transparency about data flows.* (Paragraph 36)

3. *The Government should clarify the obligations in the Online Safety Bill for voice assistants, connected devices (like smart speakers) and other emerging technologies that can surface harmful content, to ensure that those that integrate search services in particular fall in-scope of the duties. It should also set out in its response to this report how the online safety regime will categorise voice assistants and connected devices that integrate internet search so that they do not service harmful content like hate speech and other harms.* (Paragraph 41)

4. The use of connected tech in schools and by children in homes raises concerns, including the harvesting and third-party use of children's data and their lack of control over what technology is used and when. The Government and ICO were quick to dismiss our concerns about this issue. *We urge the ICO to take a more proactive approach in engaging with manufacturers of connected toys and education technology. It should ensure that all products include: terms and conditions that are age-appropriate; privacy settings that are intuitive for children and help them exercise data rights; and fully explain the benefits and risks of data processing. Industry should be supported in this through comprehensive guidance, independent research and user-testing.* (Paragraph 51)

5. *The Government should commit to ensuring that the Age-Appropriate Design Code is strengthened rather than undermined by data protection reform and to laying the revised code as soon as is practicable.* (Paragraph 52)

6. Though smart cities provide a range of opportunities, such as more efficient management of resources, there are also additional risks to confidence in privacy and data protection, making it harder for individuals to exercise data rights. *The Government should review how it can incentivise and actively pilot the creation of data institutions, in partnership with local government and other local stakeholders,*

in smart cities to address issues of data protection and ensure that citizens can have greater control over, and directly participate in the benefits from, the use of their data. (Paragraph 59)

7. The monitoring of employees in smart workplaces should be done only in consultation with, and with the consent of, those being monitored. *The Government should commission research to improve the evidence base regarding the deployment of automated and data collection systems at work. It should also clarify whether proposals for the regulation of AI will extend to the Health and Safety Executive (HSE) and detail in its response to this report how HSE can be supported in fulfilling this remit.* (Paragraph 64)

8. *The Information Commissioner's Office should develop its existing draft guidance on "Employment practices: monitoring at work" into a principles-based code for designers and operators of workplace connected tech.* (Paragraph 65)

9. The Government has not yet made a compelling case for reform of data protection. While we understand that some companies do not share data outside the UK, we are concerned that differing expectations between those companies and companies that do share data outside the UK may give the impression of "lesser" protections for processing personal data in the UK overall. This could be perceived as undermining our existing data adequacy arrangements and ultimately harm companies that share data between the UK and other jurisdictions. *To maintain the UK's reputation as a world-class technology hub, the Government should keep its data reforms under review so as not to undermine its existing data adequacy agreements.* (Paragraph 72)

10. We agree that reforming the governance and accountability structures of the Information Commissioner's Office will be a positive step. *We have previously recommended against executive overreach in the case of Ofcom and the Online Safety Bill; these concerns apply with respect to the Information Commissioner's Office and the Data Protection and Digital Information (No. 2) Bill. Powers to veto codes of practice and to set strategic priorities without parliamentary oversight should not be adopted.* (Paragraph 78)

Product security

11. The introduction of the product security regime, which codifies three of the original thirteen guidelines set out in the Government's internationally recognised 2018 Code of Practice for Consumer IoT Security, is an important first step in improving cybersecurity for connected devices. However, the remaining ten guidelines retain considerable support among stakeholders. *We recommend that the Office for Product Safety and Standards (OPSS), as the national regulator, should produce an implementation plan so policymakers can measure the impact of the product security regime. The OPSS should continue to promote the guidelines not included in the Product Security and Telecommunications Infrastructure Act 2022 and the Government should commit to codifying these remaining guidelines in phases as the regime matures and industry adapts, in order to stay ahead of emerging cyber threats.* (Paragraph 101)

12. As the guidelines set out in the 2018 Code of Practice for Consumer IoT Security imply, cybersecurity and data protection are mutually reinforcing. Without cybersecurity, data cannot be meaningfully protected, while data protection can manage the risk and impact of cyberattack. *The Information Commissioner's Office, either bilaterally or through the Digital Regulation Co-operation Forum, which helps co-ordinate regulation of digital platforms and services, should work with the Office for Product Safety and Standards as it promotes the guidelines pertaining to data protection and data security in the 2018 Code of Practice.* (Paragraph 102)

13. Improving cybersecurity of consumer connected devices is an important and positive step, but the proliferation of connected tech in enterprise settings and the gap in the regime regarding network, storage and cloud security still present likely attack vectors that will continue to allow devices to be compromised. *The Government should close the gaps for both consumer and enterprise connected tech in the product security regime by requiring that providers adopt network-level, storage and cloud-based security to the same standards as it requires for connected devices.* (Paragraph 108)

14. We are concerned about the ongoing skills shortage, as recognised in both the Government and industry's regular reporting on cybersecurity skills in the labour market, and believe that the shortage will be exacerbated further as the product safety regime comes into force. We support industry's calls for the Government to do more to address this issue. *The Government should also take steps to support the availability of free courses across the country, encourage more professionals to become cybersecurity educators, improve the provision of core professional skills among the existing workforce and incentivise industry to improve hiring practices and retention rates.* (Paragraph 116)

15. We are particularly concerned that, despite the shortage of cyber skills in the UK, there are stubborn and significant disparities in the cyber workforce based on gender and race and ethnicity. *The Government should reflect on the significant disparities in gender and race/ethnicity in the cyber workforce and take steps to improve these divides, such as by introducing additional schemes and funding to widen the talent pool, improving the culture of and attitudes to the cyber profession both in education and work, and considering how to provide professional support for people during their career.* (Paragraph 117)

16. The creation of the Department for Science, Innovation and Technology is an opportunity to ensure a comprehensive, joined up approach to cyber policy. *We recommend that responsibilities for cyber policy is co-ordinated by the dedicated Department for Science, Innovation and Technology and that government ensures collaboration between the Department and other cyber-focused teams distributed across Whitehall. Ministers in the Department for Science, Innovation and Technology should be ultimately responsible and accountable for developing and delivering cyber policy except for national security measures.* (Paragraph 120)

17. As the prevalence of connected technology grows, so too will the demand for the National Cyber Security Centre's services. *The Government should ensure that the National Cyber Security Centre has the capacity to meet demands for its services. It should explicitly consider and address capacity issues as part of its regular reporting*

on cybersecurity skills in the UK. (Paragraph 121)

Technology-facilitated abuse

18. The Government must make tackling technology-facilitated abuse, or "tech abuse", a priority. There is little evidence to suggest that our law enforcement and criminal justice system has been equipped to deal with the problems caused by tech abuse now, let alone as connected devices become even more prevalent in future. While there is no "silver bullet" for dealing with tech abuse, the Government can do more to tackle it. (Paragraph 131)

19. *The Government's response to tech abuse should involve upskilling law enforcement to improve the criminal justice response and increasing law enforcement's and victims' and survivors' awareness of specialist services tackling violence against women and girls. The Government should also reflect on how official crime data on tech abuse can be improved to expand the evidence base for specialists, academics and policymakers in order to develop a more comprehensive, co-ordinated response.* (Paragraph 132)

20. *We want to see words from cross-sector stakeholders on tech abuse now leading to positive actions. The Office for Product Safety and Standards should, at the earliest opportunity, convene a "tech abuse working group" with stakeholders, bringing industry together with researchers, specialist support services and public services. This group should be more than just a talking shop, and draw on research to produce guidance and a code of practice that establishes best practice for manufacturers, vendors and law enforcement. The working group should report publicly through the OPSS on its progress at regular intervals.* (Paragraph 138)

Formal minutes

Tuesday 11 July 2023

Members present:

Dame Caroline Dinenage, in the Chair

Kevin Brennan

Clive Efford

Rt Hon Damian Green

Dr Rupa Huq

John Nicolson

Draft Report (*Connected tech: smart or sinister?*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 138 read and agreed to.

Annexes read and agreed to.

Resolved, That the Report be the Tenth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No.134.

Adjournment

Adjourned till Tuesday 18 July at 9.30 am.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Tuesday 19 July 2022

Silkie Carlo, Director, Big Brother Watch; **Dr Lulu Shi**, Research fellow, Oxford Internet Institute; **Dr Leonie Tanczer**, Lecturer, International Security and Emerging Technologies, UCL; **Antony Walker**, Deputy Chief Executive, techUK Q1–68

Tuesday 11 October 2022

Matt Lewis, Research Director, NCC Group; **Professor George Loukas**, Professor of Cybersecurity, University of Greenwich; **Simon Moore**, Director for Strategic Engagement, Palo Alto Networks Q69–146

Tuesday 1 November 2022

Dr Matthew Cole, Postdoctoral Researcher, The Fairwork Project; **Dr Asieh Hosseini Tabaghdehi**, Senior Lecturer in Strategy and Business Economics, Brunel University London; **Dr Efpraxia Zamani**, Senior Lecturer in Information Systems, University of Sheffield Q147–215

Tuesday 22 November 2022

Svana Gisla, Producer, ABBA Voyage; **Dr Yiyun Kang**, Associate Lecturer, Royal College of Art Q216–278

Tuesday 17 January 2023

John Edwards, Information Commissioner, Information Commissioner's Office; **Stephen Almond**, Director of Technology and Innovation, Information Commissioner's Office Q279–327

David Kleidermacher, Vice-President of Engineering for Android and Made-by-Google Security and Privacy, Google; **Leila Rouhi**, Amazon Alexa Vice-President of Trust and Privacy, Amazon Q328–369

Tuesday 31 January 2023

Julia Lopez MP, Minister of State for Media, Data and Digital Infrastructure, Department for Culture, Media and Sport; **Erika Lewis**, Director, Cyber Security and Digital Identity, Department for Culture, Media and Sport; **Sam Cannicott**, Deputy Director and Head of the Office for AI, Department for Culture, Media and Sport Q370–427

Witnesses (Sub-committee on Online Harms and Disinformation)

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Tuesday 22 September 2020

Theo Bertram, Director, Government Relations and Public Policy EMEA, TikTok Q1–141

Yuan Yang, Beijing Deputy Bureau Chief and Technology Correspondent, Financial Times, and **Rui Ma,** Creator and Co-Host, Tech Buzz China**.** Q142–175

Tuesday 13 October 2020

Dr Jiahong Chen, Research Fellow in IT Law, Horizon Digital Economy Research, University of Nottingham, **Carly Kind**, Director, Ada Lovelace Institute, and **Dr Jeni Tennison**, Vice-President, Open Data Institute. Q176–235

Tuesday 26 January 2021

Elizabeth Denham CBE, Information Commissioner; and **Paul Arnold**, Deputy Chief Executive and Chief Operating Officer, Information Commissioner's Office Q236–354

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

TEC numbers are generated by the evidence processing system and so may not be complete.

1 (ISC)² (TEC0066)

2 AMDEA (TEC0056)

3 Age Check Certification Services Limited (TEC0059)

4 Amazon (TEC0065)

5 Anonymised (TEC0002)

6 Antisemitism Policy Trust (TEC0010)

7 Basu, Dr Subhajit (TEC0037)

8 Big Brother Watch (TEC0052)

9 Buckingham, Dr Sarah (TEC0014)

10 Canhoto, Dr Ana; Professor Ashley Braganza; and Dr Asieh Tabaghdehi (TEC0018)

11 Carney, Mr Sean (TEC0036)

12 Connected Innovations (TEC0030)

13 Department for Culture, Media and Sport (TEC0054)

14 Dodson, John (TEC0038)

15 Dodson, John (TEC0022)

16 EM Radiation Research Trust (TEC0026)

17 Electrical Safety First (TEC0055)

18 Electrosensitivity UK (TEC0008)

19 Goaman, Dr Karen (TEC0042)

20 Good Things Foundation (TEC0061)

21 Horizon Digital Economy Institute, University of Nottingham (TEC0046)

22 Information Commissioners Office (TEC0051)

23 Internet Matters (TEC0044)

24 Jamieson, Mrs Gillian (TEC0015)

25 Jarvis (TEC0031)

26 Kanungo, Dr Rama (TEC0057)

27 Kenton, Mrs Amanda (TEC0033)

28 Loukas, Professor George; Professor Mina Vasalou; and Dr Laura Benton (TEC0034

29 Marshall, Susan (TEC0019)

30 Milne, Claire (TEC0041)

31 NCC Group (TEC0024)

32 News UK (TEC0063)

33 Petterson, Christina (TEC0027)

34 Physicians' Health Initiative for Radiation and Environment (PHIRE) (TEC0035)

35 Raith, Mr Stuart (TEC0003)

36 Rephain - the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (TEC0043)

37 Radiocentre (TEC0058)

38 Rebel, Tanja Katarina (TEC0023)

39 Refuge (TEC0012)

40 Rudnicka, Dr Anna; Dave Cook; and Professor Anna L Cox (TEC0050)

41 Save Us Now (TEC0032)

42 Sengul, Dr Cigdem (TEC0016)

43 Shi, Dr Lulu P.; Prof Ekaterina Hertog; and Prof Victoria Nash (TEC0039)

44 Smith, Darren (TEC0001)

45 Steward, Dr Alison (TEC0009)

46 Tanczer, Dr Leonie (TEC0021)

47 techUK (TEC0049)

48 The Centre for Care, University of Sheffield (TEC0017)

49 The Restart Project (TEC0053)

50 The UKRI Trustworthy Autonomous Systems Hub (TAS Hub); The UKRI Trustworthy Autonomous Systems Node in Resilience; The UKRI Trustworthy Autonomous Systems Node on Security; and The UKRI Trustworthy Autonomous Systems Node on Verifiability (TEC0048)

51 The University of Gloucestershire (TEC0020)

52 The University of Manchester (TEC0064)

53 Turner, Sarah; and Dr Jason Nurse (TEC0029)

54 UK Research and Innovation (UKRI) (TEC0062)

55 University of Exeter; and Coastline Housing (TEC0040)

56 Which? (TEC0045)

57 Wood, Mr John (Retired) (TEC0004)

58 Zamani, Dr Efpraxia (TEC0011)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2022–23

Number	Title	Reference
1st	Amending the Online Safety Bill	HC 271
2nd	Promoting Britain abroad	HC 156
3rd	Reimagining where we live: cultural placemaking and the levelling up agenda	HC 155
4th	What next for the National Lottery?	HC 154
5th	Economics of music streaming: follow-up	HC 874
6th	Current issues in rugby union	HC 1018
7th	Sustainability of local journalism	HC 153
8th	Appointment of Richard Sharp as Chair of the BBC	HC 1147
9th	Football governance	HC 1288
1st Special	Major cultural and sporting events: Government Response to Committee's Ninth Report of Session 2021–22	HC 452
2nd Special	Influencer Culture: Lights, camera, inaction?: ASA System and CMA Responses to the Committee's Twelfth Report of Session 2021–22	HC 610
3rd Special	Influencer Culture: Lights, camera, inaction?: Government Response to the Committee's Twelfth Report of Session 2021–22	HC 687
4th Special	Rt Hon Nadine Dorries MP	HC 801
5th Special	Promoting Britain abroad	HC 1103
6th Special	Reimagining where we live: cultural placemaking and the levelling up agenda	HC 1104
7th Special	What next for the National Lottery?: Government and Gambling Commission Responses to the Committee's Fourth Report	HC 1208
8th Special	Economics of music streaming: follow-up: Government Response to the Committee's Fifth Report	HC 1245
9th Special	The sustainability of local journalism: Government Response to the Committee's Seventh Report	HC 1378
10th Special	Appointment of Richard Sharp as Chair of the BBC: Government Response to the Committee's Eighth Report	HC 1641

Session 2021–22

Number	Title	Reference
1st	The future of UK music festivals	HC 49
2nd	Economics of music streaming	HC 50
3rd	Concussion in sport	HC 46
4th	Sport in our communities	HC 45
5th	Pre-appointment hearing for Information Commissioner	HC 260
6th	Pre-appointment hearing for Chair of the Charity Commission	HC 261
7th	Racism in cricket	HC 1001
8th	The Draft Online Safety Bill and the legal but harmful debate	HC 1039
9th	Major cultural and sporting events	HC 259
10th	Another pre-appointment hearing for Chair of the Charity Commission	HC 1200
11th	Pre-appointment hearing for Chair of Ofcom	HC 48
12th	Influencer culture: Lights, camera, inaction?	HC 258
1st Special Report	The future of public service broadcasting: Government Response to Committee's Sixth Report of Session 2019–21	HC 273
2nd Special Report	Economics of music streaming: Government and Competition and Markets Authority Responses to Committee's Second Report	HC 719
3rd Special Report	Sport in our communities: Government Response to Committee's Fourth Report	HC 761
4th Special Report	The future of public service broadcasting: Ofcom Response to Committee's Sixth Report of Session 2019–21	HC 832
5th Special	The Draft Online Safety Bill and the legal but harmful debate: Government Response to the Committee's Eighth	HC 1039

Session 2019–21

Number	Title	Reference
1st	The Covid-19 crisis and charities	HC 281
2nd	Misinformation in the COVID-19 Infodemic	HC 234
3rd	Impact of COVID-19 on DCMS sectors: First Report	HC 291
4th	Broadband and the road to 5G	HC 153
5th	Pre-appointment hearing for Chair of the BBC	HC 1119
6th	The future of public service broadcasting	HC 156
1st Special Report	BBC Annual Report and Accounts 2018–19: TV licences for over 75s Government and the BBC's Responses to the Committee's Sixteenth Report of Session 2017–19	HC 98

Number	Title	Reference
2nd Special Report	The Covid-19 crisis and charities: Government Response to the Committee's First Report of Session 2019–21	HC 438
3rd Special Report	Impact of Covid-19 on DCMS sectors: First Report: Government Response to Committee's Third Report of Session 2019–21	HC 885
4th Special Report	Misinformation in the COVID-19 Infodemic: Government Response to the Committee's Second Report	HC 894