House of Commons

Culture, Media and Sport Committee

Connected tech: smart or sinister?: Government and the Information Commissioner's Office Response to the Committee's Tenth Report of Session 2022–23

Second Special Report of Session 2023–24

Ordered by the House of Commons
to be printed 21 November 2023

HC 302
Published on 24 November 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*)

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), Natalia Janiec-Janicki (Second Clerk), Lois Jeary (Committee Specialist), Olivia Rose (Media & Communications Officer), 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 X (formerly Twitter) using @CommonsCMS

Second Special Report

The Culture Media and Sport Committee published its Tenth Report of Session 2022–23, Connected Tech: smart or sinister? (HC 157), on 7 August 2023. The Government response was received on 16 November 2023 and is appended to this report.

Appendix: Government and Information Commissioner's Office Response

Introduction

I am writing to you as chair of the Culture, Media and Sport Committee in response to the Committee's report of 7 August entitled 'Connected tech: smart or sinister?'. I would like to take this opportunity to thank you and the Committee for conducting a considered inquiry on this important issue.

I would like to sincerely apologise for the delay in responding to the Committee's inquiry. Given the breadth of important issues covered in the report, the response has been co-drafted with a number of government departments and regulators·, which has led to delays in the clearance process.

In its report, the Committee made several recommendations for government action to respond to the opportunities and risks in connected technology. In my capacity as Minister of State in the Department for Science, Innovation and Technology, I enclose the joint response from the Government and the Information Commissioner's Office (ICO) to these recommendations.

Given the breadth of subject matter covered by the Committee's report, on the Government side the response has been co-authored by the Department for Science, Innovation & Technology, the Cabinet Office, the Department for Business and Trade, and the Home Office.

As the prevalence of smart and connected technologies increases, there are immense opportunities for the UK to benefit and, as with any new technology, there are accompanying risks. Departments across government are delivering an ambitious programme of work to capitalise on these opportunities and to manage challenges. As digital technology evolves and its significance on the economy and society increases, it is vital that the Government is held to account on its approach. I would like to thank the Committee for its scrutiny and advice in this important area.

Rt Hon John Whittingdale OBE MP

Minister for Data and Digital Infrastructure

DCMS Select Committee Report - Connected tech: smart or sinister?

Introduction

The Government is grateful to the House of Commons Culture, Media and Sport Committee for the recommendations put forward by the committee Chair in response to the inquiry into Connected Technology.

This document sets out a joint response from the Government and the Information Commissioner's Office to the report.

Smart and connected technology is transforming lives in homes, workplaces and public spaces across the country, with an average of nine smart devices already in every UK household. This technology is improving connectivity, efficiency and quality of life and unlocking growth and innovation for the UK. For vulnerable groups in particular, this technology can be truly transformative - from improving digital connectivity for excluded communities to providing life-saving and low-cost assisted living. For industry, connected technology is improving productivity, fostering innovation and improving business continuity. From office printers and conference calling to huge-scale automated and smart industrial applications, businesses across the UK are utilising the opportunities of this technology to unlock growth and innovation. Towns and cities across the country are using innovative smart technologies to deliver public services, like traffic management, pollution reduction and public transport, more efficiently and at a lower cost to the taxpayer.

While connected technology provides a myriad of benefits, as with any new technology, there are risks that need to be managed. New connected devices are more complex and work in a different way to technologies of the past. This can mean that users are less aware of the risks and less able to spot the signs when a device has been compromised. Connected tech collects data in new and hidden ways, and this can lead to an erosion of user privacy if not managed properly. The need for ethical design and use is particularly heightened in the case of vulnerable communities, where tensions between monitoring and sufficient privacy protection need to be reconciled.

The Government is working with stakeholders from across the economy and society to create an environment that fosters growth while raising standards of safety and security and protecting users from harm. We have an ambitious legislative agenda that will ensure the UK's laws and regulations are streamlined, future-proofed, and facilitate secure innovation while addressing both present and future challenges. We are delivering a range of high priority policy initiatives, including reducing cyber risk at source and providing the tools for people to develop both basic and technical digital skills.

The Government is grateful to the Committee for providing much-needed Parliamentary scrutiny on this topic. Digital technologies are evolving quickly and having an ever-increasing significance in all of our lives. It is vital we maintain a system of checks and balances to ensure this growth occurs safely and securely.

We partially accept the majority of the Committee's conclusions and recommendations. Where we have not accepted the conclusions and recommendations, we have outlined the existing or planned actions that are in progress to address the issues raised by the committee.

Overview - Response to 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)

We agree with this conclusion and are addressing these issues through the UK's data protection regime. All those responsible for technology which collects and uses personal data must comply with the data protection legislation, including the principle that personal data must be processed not only lawfully and fairly, but also transparently. If people using connected technology are given clear information from the outset about how devices will use their data, it is much easier for those people to exercise their data rights, including rights to seek access to their data or to object to its further use, and also builds confidence that their data will be used appropriately. Individuals are also able to directly report organisations that fail to comply with the data protection legislation to the UK's independent data protection regulator, the Information Commissioner's Office (ICO).

The government welcomes the conclusions and recommendations the ICO made for technology providers in its Tech Horizons Report in December 2022[1]. These recommendations included, for example, ensuring high standards of privacy by default, with user-centred design of connected devices; continuing to explore approaches to transparency and data minimisation in smart spaces, and further exploring the potential of privacy enhancing technologies in the context of connected devices.

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)

We partially accept this recommendation. Articles 13 and 14 of the UK GDPR currently specify what organisations need to tell individuals when collecting and processing their personal data.There are some types of information that organisations must always provide, while the provision of other types of information depends on the particular circumstances

1 https://ico.org.uk/media/about-the-ico/documents/4023338/ico-future-tech-report-20221214.pdf

of the organisation, and how and why it uses people's personal data. Article 12 of the UK GDPR sets out that the information provided by organisations should be in a concise, transparent, intelligible and easily accessible form, using clear and plain language, particularly when addressed to children.

The ICO provides guidance for organisations on how to provide privacy information, for example at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/how-should-we-draft-our-privacy-information/

The government does not agree with being overly prescriptive in respect of privacy interfaces but does agree that people should have simple and straightforward ways of engaging with connected technology. During debates on the Data Protection and Digital Information Bill, Ministers have made it clear that cookie consent banners, for example, do not work. Often the information presented to web users is too dense or opaque for web users to understand and people often "accept all" without fully understanding what they are signing up to. That is why the government will look more closely at how we can ensure that people are given simpler and more granular choices when setting their cookie preferences. As part of this work, the government will be engaging with a range of relevant interest groups, including tech experts, regulators, groups representing internet users, privacy rights groups, browser providers and online advertisers in the months ahead to explore the key opportunities and risks within each option for enabling people to select their cookie preferences using automated technologies.

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)

We partially accept this recommendation.

The Online Safety Act will ensure users are protected from illegal content and content harmful to children when using voice assistants or other connected devices that integrate internet search.

The Online Safety Act has a broad scope that can capture a wide range of online services depending on whether they are "user-to-user" services or "search" services. The Act places new tailored duties on search services.

To the committee's point about the obligations in the Bill (now Act), regulated search services will have a duty to conduct regular risk assessments in relation to illegal content, and if relevant, content that is harmful to children. Depending on the outcome of these assessments, such services will then be required to put measures in place to (i) minimise the risk of individuals encountering illegal content and (ii) mitigate and manage the risk of harm to children.

To the specific ask about voice assistants: where a voice assistant is integrated into a regulated search service then the provider of the service will be subject to the relevant

duties imposed by the Act on search services (outlined above), and these will extend to the design, operation and use of the voice assistant. Alternatively, where voice assistants use a separate search service to obtain the results it presents to its users, that separate search service would be subject to the illegal content and child safety duties, and as such would only be able to provide search content to the voice assistant which satisfied the requirements of the Act.

These duties of care deliver strong protections to children, while respecting everyone's right to access information.

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 usertesting.** (Paragraph 51)

We do not agree with this conclusion. Since the age-appropriate design code came into force in 2021, the ICO has undertaken extensive work with industry and produced guidance to help organisations design their services to conform with the code.

The code mandates that services likely to be accessed by children must be age appropriate (standard 3), by default set to the least privacy intrusive (standard 7) and transparent about the processing (standard 4). The ICO has produced guidance on these standards, including a Commissioner's opinion on age assurance and guidance on determining whether a service is 'likely to be accessed' by a child.

The ICO published its evaluation report of the Children's code in March 2023, which highlighted the pioneering impact of the code globally, the improvements made by Information Society Services and the key role for parents and schools to play in the long term success of the code. The report did show encouraging metrics around children's understanding of the code, and more widely privacy issues.

The ICO has produced a range of specific resources on the code, including frequently asked questions on Edtech and Lesson plans and resources for schools and teachers.

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)

We agree with this recommendation. The Government agrees that the Age Appropriate Design Code is a fundamental element of the UK's Data Protection Act 2018, providing critical protections to protect children online and ensure their data rights are protected. We will ensure that forthcoming reforms to the UK's data protection regime do not undermine any aspect of the Age-Appropriate Design Code. The ICO will be updating a range of guidance impacted by changes in the Data Protection and Digital Information (No.2) Bill. It will look to make any changes and updates as soon as practical to provide

regulatory certainty, including to the code, once the Bill receives Royal Assent.

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)

We partially accept this recommendation. The Government is examining the way data intermediaries—organisations that facilitate data sharing—can enable data discovery, increase usability, manage data sharing, provide infrastructure and manage risks for those sharing and using data.

Data intermediaries and institutions can have significant potential to both help businesses to share data and to empower individuals to have greater control over their data. For instance, UK public data driven practices with which to draw insight include:

- Trusted Research Environments, such as OpenSAFELY, a secure analytics platform which was developed rapidly to answer urgent clinical questions about COVID-19.
- Commercial data exchanges, such as the Rail Data Marketplace, providing a business to business intermediary platform that provides access to real time rail information.

The Government is also working to consider and manage the security risks associated with the deployment of connected places technologies enabling the country and its citizens to benefit safely from the opportunities that they bring. As these systems move, process, and store sensitive data, as well as control critical operational technology, this technology brings unique cyber vulnerabilities that need to be managed. We work closely with local authorities and procurers of this technology, providing them with guidance, such as the Secure Connected Places Playbook, and publishing research into the state of the market and the use of connected places in the UK. To support this, the NCSC cyber security principles were developed to help local authorities understand, design, and manage their connected places securely. Any interventions to bring in data institutions will consider the risks to security that they face, including how the data and systems they are connected with may be more sensitive in aggregate and are attractive targets to adversaries.

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)

We partially accept this recommendation.

The Government is committed to supporting businesses to grow, while at the same time ensuring the protection and enhancement of workers' rights. Transparency requirements are an important part of the data protection framework, whenever processing personal data. Any workplace monitoring must be consistent with the provisions contained in data protection law. In practice, this means that for any type of personal data processing, employers must satisfy one of the lawful grounds in Article 6 of the UK GDPR which includes, but is not limited to, consent. Moreover, if the processing involves any special categories of data, then a separate condition under Article 9(2) must also be met. Special categories of data include (but are not limited to) personal data revealing racial or ethnic origin, and data concerning health, among others. The Government doesn't have any plans currently to commission research regarding the deployment of automated and data collection systems at work.

The Data Protection and Digital Information Bill seeks to clarify the safeguards that data controllers (including employers) must put in place when carrying out solely automated decision-making ('ADM') (as set out in Article 22 UK GDPR) and the rights that data subjects (including employees) have when these types of workplace technologies are deployed. The reforms ensure that these kinds of ADM activities are carried out in a fair and transparent manner, providing individuals with key safeguards. These are: the right to be provided with information about such decisions, to express their point of view about decisions, to contest them, and to seek human intervention to review and correct them.

In March, we published the AI Regulation White Paper which set out our first steps towards establishing a regulatory framework for AI. We proposed five principles to govern AI, and committed to establishing mechanisms to monitor AI risk, and coordinate, evaluate and adapt the regulatory framework as this technology evolves. We have been working closely with regulators, including HSE, on how to apply these principles in practice. We received consultation responses from over 400 individuals and organisations across regulators, industry, academia, and civil society, and will be publishing our response to the consultation later this year.

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)

The ICO plans to publish guidance for employers on employee monitoring as part of their project to produce a suite of guidance to replace the 2011 Employers Code of Practice. This guidance will sit alongside the other updated guidance for employers on its website.

The ICO published draft guidance on employee monitoring in October last year and launched a public consultation on this guidance, which closed in January this year. This will inform the final guidance, due to be published in October.

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)

We do not agree with this conclusion. The UK remains firmly committed to maintaining high data protection standards—now and in the future. The proposals in the Bill are underpinned by this commitment. The Bill includes a number of important measures to simplify the legislation, reduce unnecessary regulatory burdens on organisations and stimulate growth, but these measures are counter-balanced by robust conditions and safeguards to protect the rights of individuals.

Reform of our data protection laws is compatible with maintaining free flow of personal data from Europe and with other countries the UK has data bridges with. As the European Commission itself has made clear, a third country is not required to have exactly the same rules as the EU in order to be considered adequate. Indeed, there are fourteen countries which have EU adequacy, including Japan, New Zealand and Canada. All of these nations pursue independent approaches to data protection. The Bill is an evolution of the UK GDPR and even after our reforms have been implemented, the UK will continue to have one of the closest regimes to the EU in the world.

We maintain an ongoing dialogue with the EU on our proposals and have a positive, constructive relationship. The government will continue to work with the EU and other international partners to ensure that existing free flows of data remain unaffected, to our societies' and economies' mutual benefit.

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)

We do not agree with this conclusion. The government is committed to maintaining the ICO's independence, whilst also ensuring that it is equipped to regulate effectively. The Information Commissioner himself made clear in giving his evidence to the Public Bill Committee that he feels that our reforms are compatible with that. He stated "I do not believe it will undermine our independence at all. What I think it will do is to further enhance and promote our accountability, which is very important". The SSP will ultimately be subject to parliamentary oversight, it must be laid before both Houses of Parliament and cannot be designated if either House resolves not to approve it.

Balanced alongside the proposed reforms to the statutory codes, we have set out a broad range of reforms, including requirements for published impact assessments and consultation with panels of experts, to introduce greater accountability, robustness and transparency for the ICO. The expert panels the Bill requires the ICO to establish will help the ICO assess fast-evolving uses of data and new technologies at an early stage of the process of developing new codes of practice. We expect these reforms to ensure the ICO produces effective and helpful statutory codes to support data controllers in understanding their responsibilities in complying with the law.

The Statement of Strategic Priorities will contain the government's strategic priorities for data protection and is a transparent way to provide this helpful context for the ICO. The ICO must take this Statement into account when carrying out its functions. A draft Statement will require parliamentary approval before it can be designated and the ICO will be accountable to Parliament, not the government, in its reporting on how it has considered the Statement.

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)

We partially accept this recommendation.

The proportionality of implementing a given cyber security measure for a product depends on a number of factors, from the products' technical architecture, to the setting it is ultimately deployed in. The Government is therefore mindful of the risk of imposing excessive obligations on businesses that may in many cases be disproportionate to the associated security benefits. We do not consider that there is currently evidence that it would be proportionate to mandate security requirements beyond the initial three across all consumer connectable products.

The Government will closely monitor the impact of the initial security requirements on standards of cyber security across the sector, and will not hesitate to mandate further requirements using the powers provided in the Product Security and Telecommunications Infrastructure Act if necessary.

The Office for Product Safety and Standards (OPSS), part of the Department for Business and Trade, is the UK's national product regulator. It will have responsibility for enforcement of the Product Security Regulations. OPSS' priority will be to make businesses aware of their new obligations and to tackle any non-compliance, in line with its published Enforcement Policy.

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)

We accept this recommendation. The Information Commissioner's Office will work with the Office for Product Safety Standards, either bilaterally or through the Digital Regulation Co-operation Forum, to help support one another's work, to most effectively support industry, and to ensure that enforcement of the new regulations is effective. This includes both manufacturers covered by the PSTI Act, regulated by the OPSS, and organisations who deploy technology as data controllers, covered by data protection law and regulated by the ICO.

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)

We partially accept this recommendation.

The Government is thankful to the Committee for highlighting the importance of addressing vulnerabilities in off-device elements of a product's software stack. It is not, however, correct to suggest that network, storage, and cloud security are a "gap" in the product security regime. Where appropriate, the security requirements that manufacturers of consumer connectable products will need to comply with apply not just to the physical device itself, but also software used for, or in connection with, the manufacturer's intended purpose of the product, whether it is installable on the product or not. Indeed, many enterprises will benefit from the Product Security & Telecommunications Act, as they purchase the same devices used by consumers. The Government will shortly publish our response to the recently held call for views on software resilience and security, setting out a policy approach that incorporates the evidence and views submitted by businesses and organisations.

Different categories of technology face different cyber risks, and require a different set of practices to keep them secure. We also want to make sure that the requirements are proportionate, neither placing unnecessary burdens on manufacturers, nor setting too low a bar for a certain device. As such, we take a risk-based approach to cyber policy. For example, where devices are used in critical national infrastructure, providers are required to adopt network-level security, as required by the Network and Information Systems (NIS), Telecommunications Security Act, or other CNI Regulations. Where these regulations do not apply, the NCSC recommends organisations follow the Cyber Assessment Framework, Cyber Essentials plus, Cyber Essentials or 10 Steps to CyberSecurity to secure their environments, including devices.

Further, DSIT, in cooperation with the National Cyber Security Centre (NCSC), is building a robust evidence base highlighting the cyber security risks that are present in these devices. This evidence base includes various publications, ranging from a literature review to product testing, in an effort to better understand the cyber security of these products and to examine how the Government and industry, particularly manufacturers,

can support organisations in their secure usage of enterprise connected devices. As part of this work, NCSC published a set of Device Security Principles in 2023 for enterprise connected device manufacturers. Further work is underway in DSIT to explore next steps and possible future interventions to help drive better cyber security for these devices.

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)

We partially agree with this conclusion. The Government agrees that there is an ongoing cyber skills shortage that is likely to be exacerbated as the importance of cyber security continues to increase. A priority of the National Cyber Strategy is to boost the size, quality and diversity of the UK cyber workforce. Our most recent Labour Market Survey tells us that there is an estimated annual shortfall of 11,200 people entering the field. In order to address this, the Government funds a range of cyber bootcamps through both the DfE Skills Bootcamps programme and National Cyber Strategy Programme. These are free to individual participants across the UK. This complements a range of industry-led initiatives, including the FutureLearn 'Introduction to Cyber Security' course delivered by the Open University. The Government also delivers the CyberAware campaign which looks to boost awareness and cyber hygiene best practice amongst the UK population.

The Government agrees that supporting educators is essential in order to increase access to information about a career in cyber security and technology more broadly, as well as inspiring more young people to pursue this field. We engage with like-minded countries to understand best practice, as do industry and academia across the UK.

The Government also agrees that organisations must improve their hiring practice and retention issues, given the need to close the cyber skills gap that exists. Industry is key to progress here and we will continue to engage on these topics with core industry-government groups, such as the Cyber Growth Partnership and the National Cyber Advisory Board.

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)

We agree with this conclusion. A core focus of the National Cyber Strategy is to increase diversity in the cyber workforce.

Our evidence indicates that there are not significant disparities in the cyber workforce based on race and ethnicity. Estimates from the annual survey of the UK labour market

show 22% of the cyber sector workforce are individuals from ethnic minority backgrounds, which is higher than the UK workforce breakdown of 14%. This is promising, and work with disadvantaged and underrepresented groups will continue to increase this further.

However, the gender diversity of the cyber workforce continues to be a concern. We know 17% of the cyber sector workforce is female, lower than the digital sector workforce (29%) and the UK workforce average (48%). To address this, we must inspire more young people at school to take up subjects such as computer science, where females made up only 21% of Computer Science GCSE and 15% of A level entries in 2023 respectively. The recently announced Digital and Computing Skills Education Taskforce, co-chaired by DSIT and the Department for Education, has brought together a range of industry and academic leaders to understand how we boost the number and diversity of individuals seeking a career in technology more broadly. A specific focus of this taskforce is gender diversity, and the group will produce a report with recommendations for intervention to the National Science and Technology Council in 2024.

DSIT also supports the extracurricular CyberFirst programme of competitions, summer courses and bursaries, delivered by the National Cyber Security Centre. This widens the talent pool by supporting c15,000 young people per year and is in partnership with over 200 industry employers. CyberFirst includes the DSIT 'Cyber Explorers' platform targeted at 11–14 year olds, which has reached over 50,000 students across 2,000 schools as of July 2023. DSIT also funds the 'Upskill in Cyber' programme, which saw over 3,600 applications from individuals looking to retrain or upskill in cyber, for 200 spots this year alone.

As well as inspiring and supporting individuals into a career in cyber, the Government is keen to make sure that individuals have a clear understanding of the pathways they can take to the top of their respective area. The UK Cyber Security Council, the professional body for the cyber workforce, is funded by DSIT to develop a clear process for individuals to be recognised professionally, for their expertise and experience in cyber security. This will give practitioners clarity on the knowledge, skill and experience they need to acquire over the course of their career. This structure will bring cyber security in line with more established professions, such as law and accounting. On top of this, the Department for Education has established a policy around lifelong learning to support more people to access high-quality courses that meet the skills needs of employers.

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)

We do not accept this recommendation.

The UK National Cyber Strategy 2022 sets out a whole-of-government approach, recognising that all ministers must play a role in ensuring that the UK achieves its cyber ambitions. Ministers with leading roles have specific sets of responsibilities; for example the

Secretary of State for the Home Department on response to cyber incidents, the Secretary of State for Foreign, Commonwealth and Development Affairs on work to advance UK global leadership, and the Secretary of State for Science, Innovation and Technology for the ecosystem and technology pillars of the National Cyber Strategy, as well as the cyber security of organisations in the wider economy.

Furthermore, it is not possible to separate national security measures from broader cyber policy. This is because the UK's national security is directly impacted by, and dependent upon, wider levels of cyber resilience and security across the economy and society. For example, without the right cyber skills and industrial base, good cyber resilience practices among businesses and organisations, and the embedding of security within critical and emerging technology, we will be unable to manage risks to UK national security.

Notwithstanding this whole-of-government approach, the Government recognises the need to ensure comprehensive and effective coordination and join-up, which is provided by the Chancellor of the Duchy of Lancaster (CDL), supported by the Paymaster General, via the Cabinet Office. This includes overall responsibility for the development and implementation of the National Cyber Strategy, the supporting programme of investment, and coordination of the government's efforts on cyber resilience. CDL also has overall cross-sector policy and coordination responsibility for the cyber security and resilience of the UK's critical national infrastructure.

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)

We partially agree with this conclusion.

The Government agrees that the National Cyber Security Centre (NCSC) provides vital services to the UK economy and society, demand for which will only grow as digitalisation continues. Furthermore, the NCSC's establishment simplified the government's operational structures, transformed the UK's ability to respond to national-level cyber incidents, and initiated the roll-out of innovative digital services that have helped to make organisations and individuals automatically safer online. As set out in the National Cyber Strategy 2022, the Government is ensuring that the NCSC is fit for the challenges of the next decade by clarifying the enduring capabilities and attributes that underpin its work, funding them on a sustainable basis, and focussing their use where operating experience to date tells us they will have the maximum possible impact at a national scale.

The Government is keen to ensure its annual labour market survey does not focus on any one organisation, but gives a broad sense of cyber workforce capacity across the UK. This will inform policy interventions across the wider economy, and this will also take into account the needs of the NCSC.

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)

We agree with this conclusion. This Government is determined to ensure that the perpetrators of all forms of violence against women and girls (VAWG) are held to account for their crimes—including crimes perpetrated or continued online. As technology becomes increasingly entwined with our day to day lives, it is important that we are sufficiently prepared to tackle technology-facilitated abuse and prioritise this crime type in our criminal justice response as it grows in prevalence. The 2021 Tackling Violence Against Women and Girls Strategy, and subsequent 2022 Tackling Domestic Abuse Plan, already recognise the importance of tackling technology-facilitated abuse as an integral part of the response to these crimes. Therefore, we accept the recommendation to continue to ensure that tackling technology-facilitated abuse remains a priority for this Government as part of our whole systems response to tackling violence against women and girls.

The Government is committed to addressing the differing types of technology facilitated abuse against women and girls. This includes economic abuse which is often technology-facilitated and can make an individual economically dependent on the abuser, and/or create economic instability, thereby limiting their ability to escape and access safety. In 2022, the then Minister for Safeguarding chaired an economic abuse roundtable with key stakeholders from the voluntary and financial sector to hear a range of views on how the public, private and voluntary sector can continue working together to strengthen our response to economic abuse which is often facilitated by the utilisation of tech by perpetrators. A subsequent roundtable has been held in July 2023 by HM Treasury to continue working with key partners to address the issues caused by economic abuse, including when it is technology-facilitated.

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)

We partially agree with this conclusion. We agree with the conclusion that robustly tackling technology-facilitated abuse requires policing and criminal justice partners to develop the specialist capability and skills needed to address this issue. The National Policing VAWG Taskforce has already identified technology-facilitated violence against women and girls (VAWG) as a key priority in the Strategic Threat and Risk Assessment on VAWG published earlier this year. In the assessment, they set out expectations for police forces to recognise the emerging role of technology in VAWG crimes and prioritise improving their response. It is important to note that policing is operationally independent of the Government, however, the Government will continue to work closely with policing partners such as the National Police Chief's Council and the College of Policing to ensure that police forces have the right skills, capabilities and training resources they need to respond to this emerging and evolving threat.

The Government recognises the importance and valuable expertise of specialist services in supporting victims and survivors and upskilling criminal justice partners. The Government continues to fund specialist organisations to deliver the tailored support that victims and survivors of VAWG offences and domestic abuse need. In July 2023, the Government announced up to £8.3 million will be provided to organisations across England and Wales to fund frontline and specialist support projects for victims and survivors over two years, including counselling, training and community outreach. As part of this, Refuge will receive funding to work collaboratively with specialist by-and-for organisations to support them in responding effectively to the risks of technology facilitated abuse through training.

The Government also continues to invest in vital helplines to support victims of abuse, including providing £150k in 2023/24 to the Revenge Porn Helpline to support victims of non-consensual intimate image sharing, colloquially known as 'revenge porn'.

The Government accepts the ambition of the recommendation to improve official crime data on technology-facilitated abuse. The Government will continue to work with police forces to ensure accurate use of the 'online flag' within crime data to inform policy making.

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)

We do not accept this recommendation.

The Office for Product Safety and Standards (OPSS) is responsible for regulating a range of products to ensure that they are safe and secure, as per their duties as regulator for the Product Security legislation. Therefore there are currently no plans to set up a new group by DSIT, or under OPSS in its role as the enforcement authority for the new product security regulations, to examine tech-enabled abuse. As the legislation requires manufacturers to comply with security requirements that reduce the risk of unauthorised access, this may also have a positive impact on protecting consumers from tech abuse. Aspects of tech abuse are instead addressed in several different UK Government policies and legal frameworks, including domestic abuse law, online safety policy as well as the policy on the security of IoT devices. OPSS will work closely with other Government Departments and stakeholders to ensure that any wider issues that arise from its regulatory role can be taken into account in any further policy development across Government.