BIG BROTHER WATCH

Big Brother Watch's written evidence for the Digital, Culture, Media and Sport Committee inquiry into Connected tech: smart or sinister?

June 2022

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Authors

Silkie Carlo

Elena Casale

Contact

Silkie Carlo

Director

Direct line: 020 8075 8478

Email: silkie.carlo@bigbrotherwatch.org.uk

INTRODUCTION

1. We welcome the opportunity to submit evidence to the Committee's inquiry into connected technology.
2. 'Connected technology' means any technology connected to the internet or similar digital networks, also known as the Internet of Things (IoT): physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the internet or other communications networks.[1] By 2050, there will be an estimated 24 billion interconnected devices in the world.[2] These devices are set to enter each sphere of life: our bodies, homes, cities, workplaces, and industries.
3. Such connectivity can be highly innovative, but also often creates risks of intrusive data collection, surveillance and hacking. As an organisation that seeks to protect privacy in the UK, this is a great concern for us and as such our submission aims to describe this problem and potential solutions. Our lives are increasingly oriented around connected technology – from our smart phones, to smart TVs, virtual assistants and smart speakers, fitness trackers and city sensors. Data about us is constantly being collected and processed, and our data rights are in the hands of private companies we may not even know about.
4. The mass monitoring of data that connected technology allows for will has and will lead to the manipulation of human behaviour. The 2018 book by Shoshana Zuboff, 'The Age of Surveillance Capitalism', addresses the ways in which data is used not just to monitor us but to direct and control what we do. Personal data is extremely valuable, and companies can exploit it by using it to develop behavioural models that map our desires in high resolution to target them with even greater efficiency. It is unclear that these risks have been fully accounted for by policy makers and legislators.
5. As connected technology becomes increasingly prevalent, our modern world is becoming an environment of ambient surveillance. This is a major change that will undoubtedly have serious impacts, some of which may be unforeseen or unintended.
6. **The most important impacts of increasingly prevalent connected technology are the erosion of privacy, security risks, and inequality.**
7. Almost any instance in which two or more devices connect over the internet or another network carries some risk of unauthorised or unwanted

1 Gillis, Alexander (2021). "What is internet of things (IoT)?". IOT Agenda.
2 Ericsson "https://www.ericsson.com/en/internet-of-things"/

privacy loss for the user or those around them. This may be through commercial data collection, criminal activity, exploitative or abusive use of the technology, or even state surveillance. The risk significantly varies according to multiple factors including domestic laws, product design and security measures.

8. To illustrate the range of privacy risks associated with connected technology, we can examine various privacy risks associated with smart devices that are increasingly common in the privacy of people's homes.

CONNECTED TECHNOLOGIES IN THE HOME

9. 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 can capture audio from up to 20m away. This has led to legal disputes[3] and some individuals will understandably be concerned about their neighbours' uses of surveillance devices. **Individuals using such smart devices are data controllers, quite rightly adopting legal obligations under the Data Protection Act that they may not be fully aware of.**
10. In recent years, several UK police forces have entered agreements with Amazon to promote Ring doorbells – for example, offering discount codes to members of the public on their social media pages, or distributing free devices.[4] Some police forces, such as Wiltshire Police, have asked residents to register their smart doorbells with the force so they can be called on to provide footage should police request it.[5] This may be well-intended, but appears not to consider the adverse impacts, nor the appropriateness of public authorities promoting commercial data collection products.
11. Meanwhile, in 2018 Lancashire Police partnered with Amazon to issue crime updates and safety notifications to Amazon Echo owners, and even

---

3 https://www.theguardian.com/uk-news/2021/oct/14/amazon-asks-ring-owners-to-respect-privacy-after-court-rules-usage-broke-law

4 https://www.google.com/url?sa=D&q=https://bigbrotherwatch.org.uk/2019/09/the-times-police-partnerships-with-amazon-over-front-door-surveillance-devices/&ust=1656757020000000&usg=AOvVaw19NYekUHSXXCfy4qulRhjO&hl=en-GB&source=gmail

5 https://www.telegraph.co.uk/politics/2020/03/29/police-recruit-householders-create-network-doorbell-cameras/

aimed to receive crime reports via the voice assistants.[6] This raised serious questions about third-party data storage and the anonymity of crime reports.

12. Further, in 2019 the NHS partnered with Amazon to encourage people to seek health advice from Amazon Echo devices.[7]On our analysis, encouraging the public to give their private health details to one of the most aggressive corporate data collectors was astonishingly misguided. Amazon's Alexa records what people say and stores recordings in data centres we know very little about, whilst the company exploits users' data for profit. Any risk of people being profiled and targeted by data brokers based on their sensitive, personal health concerns could compromise people's trust in medical confidentiality and as such, make healthcare less accessible.
13. **We should be cautious of blurred lines between public and private data collection and the impact on privacy.** In the US, Amazon has over 1,800 partnerships with law enforcement agencies and can request direct access to many users' Ring camera footage without a warrant, with some figures showing over 1,900 police requests for footage being made per month.[8] In 2020, we warned that the beginning of police involvement with individuals' smart doorbells in the UK risked creating "a citizen-run police surveillance network" of enormous proportions.[9]
14. **We are concerned not only about authorities' involvement in private connected technology, but also data collection by the manufacturers and other commercial interests.** As with many companies selling connected tech, Amazon's privacy policies are lengthy, vague, and very enabling for the company.
15. For example, in relation to the company's storage and processing of Ring doorbell data, the policy gives little more clarity to the user other than that the company may do so where it has a legal basis to. Some of the categories of data collected include geolocation, live video or audio streams, "data about your interactions with our websites and mobile apps", "motion, events, temperature and ambient light", social media data

---

6 https://theintercept.com/2018/03/09/amazon-echo-alexa-uk-police/

7 https://bigbrotherwatch.org.uk/2019/07/big-brother-watch-statement-on-nhs-amazon-partnership/

8 https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us

9 https://www.google.com/url?sa=D&q=https://bigbrotherwatch.org.uk/2020/03/the-telegraph-a-citizen-run-police-surveillance-network/&ust=1656757020000000&usg=AOvVaw3tWUbb_35Nk1WcymSkTB_y&hl=en-GB&source=gmail

and much more.[10] A BBC investigation in 2020 found that among the significant amount of data Amazon collects from Ring doorbell users, "Amazon keeps records of every motion detected by its Ring doorbells, as well as the exact time they are logged down to the millisecond."[11] Such granular data collection can be used to build profiles of users, social patterns and information about when they are or are not at home. In fact, the granularity of the data collected could in theory locate the position of the device to the nearest 0.00001mm. As privacy expert Frederike Kaltheuner remarked, "this isn't just about privacy, but about the power and monetary value that is attached to this data."[12]

16. Data is not only aggregated by companies but may also be directly watched or listened to. The Intercept has previously reported that, in 2016, Ring provided its research and development team "virtually unfettered access to a folder on Amazon's S3 cloud storage service that contained every video created by every Ring camera around the world."[13]
17. Likewise, whistleblowers from Amazon[14] and Apple[15] have separately revealed that voice-activated assistants regularly transmit unauthorised audio data due to trigger errors, capturing recordings of confidential, sexual, medical and illegal interactions that are listened to by company staff. Individuals fitting smart devices with live microphones in their homes entrust their private interactions to the hands of private companies whose products and policies are often highly opaque about data flows and security.
18. It is not only data flows and software processes that can be shrouded in commercial secrecy where connected technologies are concerned, but internal hardware functions too. In 2019, it emerged that a Nest security system contained a hidden microphone that was not detailed in the product specifications.[16] Many connected devices, from TVs to smoke detectors, now contain microphones with listening functions.
19. Decisions to use such smart devices in and around the home should not be viewed as purely personal decisions. They can also impact family members, visitors, post and delivery workers, neighbours and

10 https://en-uk.ring.com/pages/privacy-notice
11 https://www.bbc.co.uk/news/technology-51709247
12 Ibid.
13 https://theintercept.com/2019/01/10/amazon-ring-security-camera/
14 https://www.thesun.co.uk/tech/9611689/outrage-as-amazons-alexa-listens-to-brits-having-sex-rowing-swearing-and-sharing-medical-news/
15 https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings
16 https://www.telegraph.co.uk/technology/2019/02/20/google-failed-tell-users-hidden-microphone-nest-security-system/

neighbourhoods, and incur data protection responsibilities in relation to those people. A loss of privacy can be felt not only on a personal level but by a community.

20. **Children may be particularly vulnerable to data exploitation and security vulnerabilities, even in the home.**

21. As the National Cyber Security Centre has warned,[17] and as countless case studies have regrettably shown over recent years, smart audiovisual baby monitors with default passwords or outdated software can be easily hacked by criminals. [18] In some cases, predators have exploited audio functions to speak to children by hacking these devices. In another case, a bluetooth and internet connected "smart" doll was hacked, allowing hackers to speak directly to children.[19]

22. The growth of education technology ('EdTech'), particularly since the unprecedented rise of remote schooling during the pandemic, also puts children's data privacy at risk. In an expert, international, technical and policy analysis of 164 EdTech products by Human Rights Watch published in May 2022, 146 (89%) appeared to "engage in data practices that put children's rights at risk, contributed to undermining them, or actively infringed on these rights".[20] The rights group found: "These products monitored or had the capacity to monitor children, in most cases secretly and without the consent of children or their parents, in many cases harvesting data on who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use."[21] **Where public authorities endorse such technologies, or in some cases even require their use as part of an educational programme, they may be violating children's privacy rights and putting them at risk of data exploitation.**

23. **Likewise, disabled and elderly people may be particularly at risk of data exploitation associated with connected technologies in the home.**

24. As with digital education, there has been a shift towards digital social care in light of austerity measures and subsequently, the pandemic. 'Telecare',

---

17 https://www.reuters.com/article/us-britain-cybercrime-technology-idUSKBN20Q1OH

18 https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home

19 https://www.bbc.co.uk/news/world-europe-39002142

20 How Dare They Peep into My Private Life?"Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic – Human Rights Watch, May 2022: https://www.hrw.org/sites/default/files/media_2022/06/HRW_20220602_Students%20Not%20Products%20Report%20Final-IV-%20Inside%20Pages%20and%20Cover.pdf

21 Ibid.

for example, involves UK councils installing sensors and alarms in vulnerable people's homes that, when triggered, call the Telecare call centre for assistance.[22] Many aspects of Telecare offer significant advantages and can include fall alarms, either at the home level or personal alarms, and flood alarms that alert someone if a bath overflows. It can allow people a greater degree of independence and it can facilitate a vulnerable person staying in their own home longer than they may otherwise would.[23] However, potential privacy infringements must be considered, as must the ethics of increasingly remote health and social care. **Connected technologies may not always be a suitable replacement for human care for vulnerable people.**

25. During the pandemic, shielding policies and moves to limit the social contact of clinically vulnerable groups led to many local authorities turning to Telecare options.
26. British company Alcove, for example, signed a number of contracts with local authorities in the wake of the pandemic to install its CarePhone, including one to install the devices in 5,000 homes across Essex, Sussex and Kent.[24] According to Kent County Council's responses to our 2020 Freedom of Information requests, the device is a video-enabled tablet computer that allows calls between the individual and their carers, family, friends and other approved numbers in a person's support network, via a SIM card (rather than relying on WiFi). The devices were offered to people who required 10 hours or less of care per week.
27. Alcove also offers a number of other products, such as glucose measures and in-home sensors, but at the time of our research they were not linked to the tablets in this 5,000 device project.
28. Use or a lack of use of the tablets was monitored by Alcove and the company was notified if the device was unused or turned off, when it was then is either able to call the user or ask someone in their support network to do so. Information about this was then given to the council to make any changes to care plans.
29. Significant amounts of other data were gathered by Kent County Council such as detailed call records including time and date, length, type and who was called. Alcove was also given significant personally identifiable

22 https://hackney.gov.uk/telecare

23 https://www.ageuk.org.uk/information-advice/care/housing-options/adapting-home/telecare/

24 https://www.youralcove.com/blogs/news/local-government-association-article-essex-kent-suffolk-county-councils-groundbreaking-5-000-covid-19-videocarephone-rollout

information about the care receivers who have a device, including their name, gender, contact details and information about their care provider.

30. Any friends or family who wished to contact a relative via the tablet were also required to log in through Alcove's online portal and provide their personal details to the company, including their name, phone number, email, IP address and analytics from their web browser.

31. The Data Protection Impact Assessment further suggested that significant amounts of sensitive data and information about vulnerable subjects would be collected and processed. Personally identifiable information would be visible on reports generated about the Carephone project such as age, postcode and an identifier number - which could be enough for jigsaw re-identification. It was claimed that this was needed for analysis and risk would be mitigated by encryption. It is important to consider that the potential privacy risk is amplified by the vulnerability of the people who are the subjects of this trial.

32. Participation in the Carephone programme was optional. However, Kent County Council said carers would "strongly recommend" vulnerable individuals accept the tablet during the pandemic. People receiving a Carephone were given a summarised privacy policy and informed that the full policy was available online. The asymmetry of power in this situation should be noted when considering whether consent is freely given. That said, Kent County Council relied on a "public task" legal basis for the data processing rather than consent, noting the public health exemption for special category data.

33. Kent County Council was explicit in stating it planned to use the tablets to cut in-person visits and benefit staff by "reducing travel time and unnecessary visits", while allowing more to be done with fewer staff. It is unclear whether the council accounted for the harms of reduced social contact.

34. Remote care via connected technologies should not be seen as a complete substitute for in-person contact. Studies into adults suffering from chronic pain found that Telecare should serve to augment rather than replace in-person care for it to benefit individuals.[25]

35. Other local authorities, such as Hampshire Council, used Amazon Alexa devices as a social care solution. The project involved both ordinary use of the devices and the development of bespoke apps to work in a social care

25 Social Isolation And The Perceived Importance Of In-person Care Amongst Rural Older Adults With Chronic Pain: A Review And Emerging Research Agenda, A Mort et al, January 2014, Journal of Pain Management. 7(1)

setting. The intrusion of one of surveillance capitalism's biggest players into the homes of vulnerable people and the lack of added protections in light of this was alarming.

36. Hampshire County Council documents we obtained showed that the person receiving care was required to set up an Amazon account to use a device, which was provided by the authority's care technology outsourcer, Argenti. The voice assistant was intended to support reminders and appointment planning, contact with friends and family, and control over lights and other connected appliances. Users were informed that Amazon may use their data for marketing purposes, and referred to the company's 4,000 word privacy policy for further details.
37. Whilst promising benefits, public duties such as social care and education being conducted increasingly via connected technologies have **the potential to usher in a low-contact, data-exploiting relationship between citizens, private companies and the state.**
38. **Public authorities should undertake privacy audits of connected technologies they contract and/or promote, and minimise data collection to that which is necessary only. Authorities should not contract or partner with technology providers who are unwilling to minimise data collection.**
39. **Furthermore, the use of connected technologies should ideally be an option that individuals can consent to, rather than an enforced replacement for human contact.**
40. Other groups may be at particular risk of connected technologies in the home.
41. **In particular, women and other people living in coercive, controlling or violent households are at risk of interpersonal data exploitation associated with connected technologies in the home.** We would refer the Committee to the pioneering work of Dr Leonie Tanczer and colleagues working on the Gender and IoT project at UCL, who have amassed a wealth of evidence and analysis of the impact of connected technologies on gender-based violence and abuse.[26]

CONNECTED TECHNOLOGIES IN OUR CITIES

42. Connected technologies are increasingly used in our towns and cities, and the futuristic notion of "smart cities" is now an emerging reality.

---

26 https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot

43. Smart cities have the potential to be operationally and environmentally efficient and provide fast connectivity for the public, but they also have **the potential to be extreme surveillance environments**. Further, they may incur serious security risks.
44. Some connected technologies may be repurposed for a function they were not initially intended for. 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.[27] Although we wrote to the Government requesting further information, very little information was made public about this data processing.

CONNECTED TECHNOLOGIES IN THE WORKPLACE

45. Sensors and other connected technologies have become increasingly popular in workplaces.
46. In 2018, the TUC published an important report on workplace monitoring, titled 'I'll be watching you'.[28] The report found that over half of workers (56%) thought it's likely that they're being monitored at work and 66% were concerned that workplace surveillance could be used in a discriminatory way if left unregulated.
47. In February 2020, we discovered that Barclays had introduced desk sensors that tracked the time employees spent at their desks, sending warnings to those deemed to have taken long breaks. Intrusive monitoring denies staff the privacy, respect and dignity they deserve at work. We publicly urged Barclays to scrap the surveillance system, which they very soon did.[29] However, we believe similar systems are likely to be common in many workplaces.
48. The rise of home-working during the pandemic also led to an increase in surveillance technologies being imposed on employees within their own homes. Microsoft even filed a patent for a system to monitor employees' facial recognition and body language to assign productivity scores to employees.[30] Such "engagement" analysis is emerging in both workplace

---

27 https://bigbrotherwatch.org.uk/2020/10/government-funded-artificial-intelligence-cameras-and-sensors-used-in-uk-towns-to- monitor-social-distancing/

28 https://www.tuc.org.uk/research-analysis/reports/ill-be-watching-you

29 https://bigbrotherwatch.org.uk/2020/02/city-am-barclays-scraps-big-brother-staff-tracking-system/

30 https://bigbrotherwatch.org.uk/2020/12/bbc-microsoft-has-filed-a-patent-for-a-system-to-monitor-employees-facial-recognition-and-body-language/

and education environments, relying on the false premise that there is a uniform, normative way that people work optimally.

49. A 2021 report by the Joint Research Centre (JRC), the European Commission's science and knowledge service, warned that excessive employee monitoring whether in the workplace or in remote working contexts has negative psycho-social consequences including increased labour resistance, stress and turnover propensity, along with decreased job satisfaction and organisational commitment. The study also found that "The surveillance of employees working remotely during the pandemic has intensified, with the accelerated deployment of keystroke, webcam, desktop and email monitoring in Europe, the UK and the USA."[31]
50. Similarly, a 2021 report by The All Party Parliamentary Group on the Future of Work found that there had been a marked increase in the use of AI technologies in the workplace and that beyond the usual concerns around surveillance, pervasive monitoring and target setting technologies were associated with pronounced negative impacts on mental and physical wellbeing.[32]
51. **It is important for individuals' autonomy, dignity and health that the home remains a private space, free from intrusive employer surveillance via connected technologies.**

CONNECTED TECHNOLOGIES IN SCHOOLS

52. Connected technologies are becoming more frequently used in classrooms; from direct monitoring through biometrics to facial recognition and tracking technologies to iPads and smart whiteboards.
53. A major issue with the use of such technology in the classrooms is that young children cannot conceivably give free and informed consent to the use and processing of their personal data. Children are particularly vulnerable when their data is being collected and processed as they may be less aware of the risks involved.
54. This has been affirmed in the European case law relating to the use of facial recognition in schools. In February 2020, the French administrative court held the use of facial 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 student, the

31 https://publications.jrc.ec.europa.eu/repository/handle/JRC125716
32 https://www.futureworkappg.org.uk/news/zownl0mx4t4n6smrk4dmzor0oz4djg

inherent power asymmetry in the school environment means consent can never be given to use of facial recognition in schools under the GDPR.

CONNECTED TECHNOLOGIES AND INEQUALITY

55. We have identified risks for uneven impacts of connected technologies throughout this submission across different groups. **Children, older people, disabled people, women, and workers on low incomes are all disproportionately affected by the adverse impacts of connected tech.**
56. Further, the impact of the digital divide must be considered. Older people and people on low incomes can be shut out of the modern, and future world. This has been a particular issue in the context of the digitisation of banking and welfare.
57. Looking ahead, the deployment of smart devices across every stratum of society further risks creating mass unemployment. Estimates of the proportion of jobs in the UK that could, over the next two decades, be replaced by artificial intelligence and related technologies range from some 22% to between 40% and 45%. The rise of smart factories, and intelligent and flexible automation, will make manufacturing cheaper, quicker, more efficient, more personalised, and more reliable. As wealth becomes increasingly concentrated in the hands of businesses that employ fewer and fewer humans, society may face renewed inequality.

CONNECTED TECHNOLOGIES AND SECURITY RISKS

58. The security risks of fully connected public and private environments must be carefully considered.
59. With each new device, the 'attack surface' broadens, I.e. "the sum of vulnerabilities that are currently present on their network, both physical and digital."[33] Our vulnerability to cyberattack is set to compound rapidly as these connected technologies increase.
60. Hackers are driven by a range of nefarious motives: from financial gain (online fraud is now the most common crime in the country), to terrorism, pranking, and monetary extortion.[34]

---

33 '7 Internet of Things Threats and Risks to Be Aware of' Security Scorecard. August 4 2021.

34 Sara Sun Beale & Peter Berris, Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses, 16 Duke Law & Technology Review 161-204 (2018)

61. We are currently very vulnerable to cybercrime. When data is transferred, received, or stored through connected networks, there is often the potential for a breach or compromised data. This is often due to the lack of encryption and access controls before data is entered into the connected device ecosystem.
62. With regular security updates needed to protect devices, people often use insecure devices, not realising they are unprotected and easy to hack. Many connected devices come with default and easily identifiable passwords that hackers can exploit. One weak passcode can be all it takes to compromise a network.
63. In many cases, people have little or no way to know when their connected devices have been compromised. When the underlying software has been corrupted, the device itself often continues to function as intended, leaving little obvious reason to replace it.
64. **In the most severe cases, cyber insecurity can put human lives at risk.** Smart pacemakers and defibrillators have the potential to be tampered with if not secured properly and hackers can purposefully deplete batteries or administer incorrect pacing and shocks. Professor Kevin Fu, an expert in medical device cybersecurity, said he "fear[s] for the day where every hospital system is down, for instance, because an [IoT] attack brings down the entire healthcare system."[35]
65. The dangers of connected devices in the automobile sector were illustrated when, in 2015, hackers took control of a Jeep Cherokee through its infotainment system. They were able to "turn the steering wheel, briefly disable the brakes and shut down the engine."[36] Many computer security experts fear that the USB port at an airline seat could potentially be used to control the plane's avionics.

CONNECTED TECHNOLOGIES AND THE NEED FOR REGULATION

66. There is widespread recognition that legislation has failed to keep pace with technological developments. The Prime Minister warned in a 2019 speech, calling for greater international co-operation on data protection: "this technology could also be used to keep every citizen under round-

---

35 Hearing Before the H. Comm. on Energy and Commerce, 114th Cong. 43. (2016) (testimony of Kevin Fu), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf

36 Craig Timberg, Hacks on the Highway, WASHINGTON POST, Jul. 22, 2015, at 3, http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on thehighway/?utm_term=.f074b322c45a.

the-clock surveillance. A future Alexa will pretend to take orders. But this Alexa will be watching you, clucking her tongue and stamping her foot".[37]

67. However, his Government is now seeking to rip up data protections at home, via an anticipated Data Reform Bill that waters down Data Protection Act rights.

68. The Government's data reform plans appear to prepare the ground for an industry-tailored watering down of the bare minimum safeguards that protect individual and collective privacy from corporate and wider intrusion.

69. We are on the precipice of the greatest technological revolution in history. Data rights are not merely a technical or economic concern – they guide the path of our society's future. The data rights afforded by the Data Protection Act 2018, incorporating GDPR, are essential, minimal protections for citizens arriving at the dawn of smart cities, connected environments, algorithmic decisions, biometric surveillance, and big data grabs.

70. Data processing by connected technologies falls within the ambit of GDPR, including rights to be informed and of access, the right to rectification, the right to erasure, the right to object and restrict processing, and protections from solely automated decisions.

71. 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. **We believe the Government should use our existing data protection framework as a foundation to build upon in order to meet the growing threats of adverse impacts of connected technologies – to dismantle and weaken that foundation would be an act of sabotage that would make the UK not more but less equipped for the significant changes of our technological near future.**

72. The Public Security and Telecommunications Infrastructure Bill offers promising mechanisms for further regulation to protect individuals' security in the context of connected technologies.

73. High security standards should be implemented for connected devices in the public and private sectors. Implementing a rigorous security standard that takes privacy and security into consideration right at the start of the design process would promote privacy and allow companies diffuse the threat of cyberattacks. This security standard does not just need to be

37 https://www.theverge.com/2019/9/25/20883172/boris-johnson-un-speech-google-alexa-pink-eyed-terminators-uk-prime-minister

built in at the start; it needs to be upgradeable over time as threats evolve and compel continuous monitoring.

74. There is a high cost of not intervening imminently. Even if a high security standard were rolled out now, it would not affect the millions of existing devices that may continue to be vulnerable to attack.
75. The Bill broadly provides mechanisms rather than solutions. Therefore, its impact remains to be seen.
76. Furthermore, security is only part of the problem this inquiry is sure to identify – **commercial data collection is often built in to connected technologies by design, offering the manufacturer further commercial opportunities to profit from data exploitation. To tackle this, the UK needs strengthened data protection laws.**
77. Regrettably, the Government's intention to water-down the data protection framework offers no basis to trust that there is serious legislative intent to protect the British public from the serious harms of data exploitation arising from connected technologies, and a future world increasingly devoid of privacy that those harms entail.

Silkie Carlo

Elena Casale

June 2022