BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Big Brother Watch's written evidence to the Joint Committee on Human Rights on The Right to Privacy (Article 8) and the Digital Revolution inquiry.

February 2019

About Big Brother Watch

Big Brother Watch is a cross–party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK. We expose and challenge threats to people's privacy, freedoms and civil liberties at a time of enormous technological change in the UK.

CONTENTS

EXECUTIVE SUMMARY

- A significant challenge to the right to privacy in the digital revolution in the UK comes from state mass surveillance, the rapid and experimental adoption of new technologies in policing, and automation in public services such as the welfare system.
- We recommend that formal processes are instituted whereby public authorities seeking to adopt new technologies that engage rights in novel ways must first conduct public and parliamentary consultations.
- We believe that two important amendments are required to the Data Protection Act 2018. First, decisions that engage individuals' human rights must be never be purely automated; second, automated decisions should be more clearly defined as those lacking *meaningful* human input.
- We recommend that micro-targeted online advertising is banned in the UK.

1. INTRODUCTION

1.1 We welcome the opportunity to submit evidence to the Joint Committee on Human Rights on this important inquiry into the right to privacy and the digital revolution.

1.2 We are living through a time of seismic technological change that will reshape the world around us. In the past fifteen years, this digital revolution has already reshaped notions of privacy – both as a social good and as a fundamental right protected by law.

1.3 Our private lives are more public than ever, and our social lives are increasingly mediated by private social media companies who also profit from monitoring, collecting and exploiting our personal data.

1.4 Private companies are constructing the new digital environment in which we live, renegotiating privacy norms in the process. New technologies and 'big data' analytical systems increasingly monitor and track us, feeding off our personal data.

1.5 However, perhaps the greatest challenge to the right to privacy in the UK comes from state surveillance. The right to a private life, protected by Article 8 of the European Convention on Human Rights (ECHR), is vital for maintaining a balanced relationship between the citizen and the state.

1.6 In 2013, the Snowden documents revealed that the British state had conducted domestic population-level surveillance of electronic communications, mass internet surveillance, mass webcam interception, social media monitoring, and much more. The documents revealed that new technologies have enabled states to conduct ever more intrusive monitoring, whilst making citizens ever more vulnerable to intrusion. The emergence of mass surveillance in a democratic society constitutes an unprecedented and serious threat to the right to a private life.

1.7 Further challenges to citizens' right to a private life are fast evolving, and the actions of states and private companies are often closely linked. The public sector is rapidly adopting commercial software, either replacing human functions or introducing new processes. This includes machine-learning, predictive policing systems; artificial intelligence (AI) facial recognition surveillance software; AI recidivism risk tools fuelled by marketing data; automated risk assessments and 'Voice Risk Analysis' for welfare applicants; and digital evidence software, including AI analysis, in the criminal justice system.

1.8 Therefore, one cannot accept at face value the proposal in this inquiry's terms of reference - that it is "private companies which provide digital infrastructure, products and services that have the greatest impact on (privacy rights)".[1]

---

1 Data collection by private companies: a threat to human rights?
https://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/news-parliament-2017/right-to-privacy-digital-revolution-launch-17-19/

1.9 Big Brother Watch seeks to protect the right to privacy in the face of these evolving challenges through parliamentary lobbying, public campaigns, and litigation. However, even parliamentary and legal processes have failed to adequately protect the right to privacy.

1.10 Government must set a good example and provide leadership through this digital revolution. The parameters for privacy norms are, in large part, set by government through its respect for citizens' privacy, its adoption of technologies, and the laws and regulations it puts in place. Therefore, in this submission we will focus on the state's adoption of new rights-altering technologies, their impact on citizens' rights, and the strength of relevant laws and regulations. In particular, we will address those technologies used in UK policing and the welfare system.

1.11 We do not address investigatory powers any further in this submission as that matter requires an inquiry of its own; the Investigatory Powers Bill was previously examined by the Committee, and the Act is now subject to judicial review – but we trust we have made our view clear that it presents one of the most profound threats to the right to privacy in the UK since its enshrinement in UK law.

1.12 Never before has the human rights framework been challenged by such a significant technological and societal transformation – and this is just the beginning. The question of whether Article 8 can sufficiently protect the right to a private life in an environment where technological capabilities, state surveillance and the very notion of privacy itself have so radically shifted remains to be seen. However, we strongly believe that it can, and resolutely campaign for its protection – but the right decisions have to be made now.

2. PRIVACY, RIGHTS & TECHNOLOGIES IN UK POLICING

Live facial recognition technology

2.1 One of the most privacy-altering technologies to enter UK policing is live facial recognition, which has been gradually deployed since 2015.

2.2 The technology was introduced to the UK with a complete lack of transparency, public or parliamentary consultation, or legal basis. Big Brother Watch has been investigating and publicising its use by police,[2] and we are now bringing a judicial review against the Metropolitan Police and the Home Office

2.3 The artificially intelligent live facial recognition technology being used has been bought from a Japanese company NEC.[3] The software analyses CCTV feeds to scan the faces of every individual within the camera's range, creating unique biometric maps of their faces and comparing their 'faceprints' to secret police watch lists of images,[4] similar to a fingerprint check.

2.4 Watch lists are drawn from the custody image database, which itself raises significant privacy issues, stemming not just from emerging technology, but out-dated technology. There are 19 million custody images on the Police National Database,[5] including thousands of people who were never charged, or found not guilty. The Biometrics Commissioner estimated that hundreds of thousands of images on the Police National Database are of innocent people.[6] The outdated database does not hold integrated data on individuals' criminal justice outcomes and cannot support automated deletion for innocent people. Whilst failing to resolve this elementary problem and breach of rights,[7] the system was upgraded in 2014 to make 12.5 million custody images biometrically searchable using facial recognition.[8]

2.5 Facial recognition can be compared to a fingerprint scan – but in a live setting, with public surveillance cameras, it differs significantly in that it is a non-contact, non-consensual and semi-covert process that is applied indiscriminately to the whole crowd in view of a camera. Clearly, this technology enables identity checking and tracking on an unprecedented scale.

---

2 Big Brother Watch (2018), 'Face Off: the lawless growth of facial recognition in UK policing', 15th May 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf)

3 https://www.nec.com/en/global/solutions/safety/face_recognition/NeoFaceWatch.html

4 https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/

5 Press Association: 'Custody image' deletion request figures revealed, 12 February 2018 (http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.htm)

6 BBC News Online, 'Facial recognition database 'risks targeting innocent people', 14 September 2018 (http://www.bbc.co.uk/news/uk-41262064)

7 *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)

8 Science and Technology Committee: Oral Evidence – Biometrics Strategy and Forensic Services, HC 800, 6 February 2018. (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/biometrics-strategy-and-forensic-services/oral/78113.htm)

2.6 Our investigation found that police facial recognition surveillance has so far misidentified innocent people up to 98% of the time, with an average of 95% of people 'matched' in fact misidentified.[9] As this is AI technology, NEC's algorithm learns and improves by using British citizens as guinea pigs for this technology, raising novel ethical and legal questions.

2.7 The NEC NeoFace software used by the police has not been tested for demographic accuracy biases, despite widespread concerns arising from multiple studies showing that facial recognition technology can disproportionately misidentify people of colour and women.[10] As a commercial technology, it is unclear whether NEC or police forces should be responsible for such testing. In any event, police forces ultimately bear responsibility for ensuring that whatever tools they use, they do not unfairly discriminate against people based on their race, sex, or any other protected characteristic. However, Article 14 ECHR may well be engaged by police use of this technology.

2.8 Such a privacy-altering technology naturally engages a multitude of rights and lends itself to abuse. The very fact of being able to biometrically check the identities of up to 300 people each second, as the NEC technology claims to do, opens the door to urban intrusion on a scale never seen before. We believe that it could never be considered necessary or proportionate in a democratic society to perform such mass identity checks and unconsented biometric processing in public spaces, and as such, that the police's use of live facial recognition breaches Article 8.

2.9 We have already observed the technology being abused. It was used by the Metropolitan Police against innocent individuals with mental health issues, despite not being wanted for any crimes,[11] and it was used by South Wales Police a peaceful protest. The use of this authoritarian identification technology clearly not only breaches privacy rights but has a chilling effect on people's right to freedom of expression and association, protected by Articles 10 and 11 respectively.

2.10 Following our report, the Information Commissioner stated that:

> "[H]ow facial recognition technology is used in public spaces can be particularly intrusive. It's a real step change in the way law-abiding people are monitored as they go about their daily lives."

---

9 Big Brother Watch (2018), 'Face Off: the lawless growth of facial recognition in UK policing', 15th May 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf)

10 Buolamwini, Joy; Gebru, Timmit: Gender Shades – Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of Machine Learning Research 81:1, p.1-15, 2018. (http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf) The study analysed the software made by Microsoft, IBM and Face++, which provides its software to the Chinese government.

11 https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph

2.11 Several major commercial technology companies have admitted that there is a need for citizens to be protected from the use of facial recognition by governments.[12] It is concerning that major facial recognition vendors have expressed more concern about the potential of their technology in government hands than governments have themselves.

2.12 Big Brother Watch continues to campaign against UK police use of facial recognition, backed by 15 rights and race equality NGOs. Despite our warnings that it breaches citizens' rights, and indeed our litigation, the Metropolitan Police and South Wales Police continue to use the technology.

Predictive policing and risk assessment systems

2.13 A number of UK police forces are investing in commercial software, or building their own systems, to predict crime.

2.14 In addition to undermining privacy and engaging a myriad of rights issues, the use of commercial machine-learning and 'black box' AI in the criminal justice system raises very serious accountability issues, as the decision-making processes cannot be understood or analysed. If an individual is subject to a decision, prediction or risk assessment, but cannot be told the reasons for the decision nor challenge it, there is an unacceptable accountability deficit.[13] In such a context, it is difficult to ensure the protection of individuals' rights and even their right to a fair trial.

PredPol

2.15 PredPol, is a geographic crime prediction tool that feeds crime and location information to a machine-learning algorithm to calculate predictions.[14] However, multiple studies have found that these systems can lead to areas being disproportionately over-policed, resulting in self-perpetuating feedback loops where predictions become self-affirming.[15] Similar systems have been or are currently being considered by Greater Manchester Police, West Midlands Police, Yorkshire Police and the Metropolitan Police. However, it is clear that these experimental predictive systems could have discriminatory impact.

Harm Assessment Risk Tool (HART)

2.16 Durham Constabulary has also developed its own machine-learning algorithm, the Harm Assessment Risk Tool (HART), which profiles suspects to predict their risk of recidivism. This AI-

12 https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/amp/; https://www.telegraph.co.uk/technology/2018/12/07/microsoft-president-calls-new-rules-facial-recognition-technology/

13 https://publications.parliament.uk/pa/cm201719/cmpublic/dataprotection/memo/dpb06.pdf

14 https://www.predpol.com/

15 Lyria Bennett Moses & Janet Chan (2018) Algorithmic prediction in policing: assumptions, evaluation, and accountability, Policing and Society, 28:7, 806-822, DOI: 10.1080/10439463.2016.1253695 ; Ensign et al, (2017) 'Runaway Feedback Loops in Predictive Policing', Cornell University Library, 29 June 2019 https://arxiv.org/abs/1706.0984)

generated risk score is used to advise whether to charge the suspect or release them onto a rehabilitation programme.

2.17 The system is fed 34 pieces of data, including criminal record information. However, our investigation found that one of the data sources fed into the HART system is commercial marketing data from Experian, known as Mosaic. This consists of postcode stereotypes built from 850 million pieces of data, including health data, GCSE results, child benefits and income support, family and personal names linked to ethnicity, data scraped from online sources and much more. This data profiles all 50 million adults in the UK[16] into crude stereotypes based on their postcodes such as "Asian Heritage" or "Disconnected Youth".[17] Experian's profiles attribute 'demographic characteristics' to each stereotype – for example, characterising "Asian Heritage" as "extended families" living in "inexpensive, close-packed Victorian terraces", adding that "when people do have jobs, they are generally in low paid routine occupations in transport or food service".[18]

2.18 This tool raises novel questions about big data and privacy, the right to be free from profiling and automated decisions, algorithmic discrimination, and fairness in the criminal justice system – none of which have been addressed in the development of this tool. It is unacceptable that this tool, driven by profiling data, is being used by UK law enforcement systems to inform potentially life-changing criminal justice decisions. Allowing this kind of profiling data to be used risks producing unfair and inaccurate decisions and a 'postcode lottery' of justice, reinforcing existing biases and inequality.

National Data Analytics Solution (NDAS)

2.19 In addition, the new National Data Analytics Solution (NDAS), piloted by West Midlands Police but intended for all police forces to use from March 2019,[19] uses data about individuals taken from a number of public bodies to predict the risk of someone committing a crime in future, in order to pre-emptively intervene.

2.20 An independent review of the system said that there were "serious ethical issues" in particular in relation to inaccurate prediction and "the potential reversal of the presumption of innocence".[20] We share those concerns. It also raised questions around privacy rights and data

16 Mosaic Infographic, Experian, (http://www.experian.co.uk/marketing-services/knowledge/infographics/infographic-new-mosaic.html) Also see Paul Cresswell et al, 'Under the bonnet: Mosaic data, methodology and build', Experian Marketing Services, 1 April 2014, p.7: (http://www.experian.co.uk/assets/marketing-services/presentations/mosaic-data-methodology-and-build.pdf)

17 Mosaic Public Sector brochure, Experian, 2016, pp.6-9: (http://www.experian.co.uk/assets/marketing-services/brochures/mosaic-ps-brochure.pdf)

18 Mosaic UK Data Profile, Experian, 2017, p.51 (https://www.experianintact.com/content/uk/documents/productSheets/MosaicConsumerUK.pdf)

19 https://www.newscientist.com/article/2186512-exclusive-uk-police-wants-ai-to-stop-violent-crime-before-it-happens/

20 https://www.turing.ac.uk/sites/default/files/2018-11/turing_idepp_ethics_advisory_report_to_wmp.pdf

protection, specifically the repurposing of data collected by public services for policing, the accuracy of the data, and people's ability to "meaningfully consent" to their data being used.

Digital evidence

2.21 Digital evidence increasingly features in criminal investigations. Police are also using more and more advanced technology to access, download, and analyse digital evidence as part of these investigations.[21] However, technological and legal and policy limitations currently mean that digital evidence collection can be extremely intrusive, obstruct justice, and infringe rights.

2.22 This affects not only suspects but victims of crime, and has become a particular issue for victims of sexual offences. When a complainant indicates that there is digital evidence relevant to a sexual offence on a device in their possession such as a mobile phone, computer or tablet, the devices are typically taken from the complainant and the data extracted. On average, a mobile phone can contain the equivalent of 30,000 A4 pages of documents,[22] ranging through texts, emails, photos, videos, and previously deleted data, and a significant amount of extremely personal and sensitive information. Police also request logins and passwords to victims' social media accounts and personal 'cloud' storage services.

2.23 The out-dated technology in use inevitably leads to disproportionate investigations of victims' digital lives and arguably breaches their privacy rights. The data extraction software police currently use forces the download of everything within a data category, for example all messages or all photos, even if only a single message or photo is needed for evidential purposes.[23] [24] In some cases, police take an entire digital copy of all the information on a device.

2.24 **Big Brother Watch recommends that formal processes are instituted whereby public authorities seeking to adopt new technologies that engage rights in novel ways must**

21 Privacy International, 'Digital Stop and Search', 27 March 2018 (https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile)

22 Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

23 https://www.documentcloud.org/documents/4348952-MET-Redacted-Self-Service-Equipment-Kiosk-Local.html in Privacy International, 'Digital Stop and Search', March 2018 (https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf)

24 https://www.telegraph.co.uk/news/2018/03/31/police-rolling-technology-allows-raid-victims-phones-without/

first conduct public and parliamentary consultations and seek independent legal advice.

3. PRIVACY, RIGHTS & AUTOMATION IN THE WELFARE SYSTEM

3.1 In recent years, the public sector has frequently turned to the private sector for new technologies that promise to offer speed, ease and financial benefits. Local authorities are rapidly adopting commercial software to conduct automated processing and even predictive analytics, particularly for use in the complex fields of welfare and social care. This could negatively impact the UK's poorest people.

3.2 We are concerned that the use of new technologies sourced from private companies are engaging human rights in ways that are difficult to assess. The transparency, accessibility and contestability of decision-making processes appears to be largely obstructed by the adoption of commercial technologies, and in any event, is not sufficiently required by law.

3.3 Privacy rights are undoubtedly affected by the trend for ever-more digital governance. Authorities are driven to collect and analyse ever-growing volumes of data about citizens and process it in new and complex ways. However, this privacy shift is not the only way in which rights are affected by the emergence of digital technologies.

3.4 The UK's welfare system reflects principles that are at the heart of human rights frameworks: fairness, equality, and the duty of the state to ensure all of its citizens, regardless of sex, race, age, ability, or disability, enjoy a minimum standard of living. It touches on a spectrum of rights: the right to life, the right to health, the right to be free from inhuman or degrading treatment, freedom from discrimination, the right to education, the rights of children, the right to fair work, access to justice, and the right to peaceful enjoyment of property. In the context of welfare estimations and decisions, this myriad of rights is engaged and people's lives, health and social integration are often at risk.

3.5 Therefore, decision-making in this context should be transparent, comprehendible to officials and claimants, and challengeable – not just for highly trained lawyers, but for everyone, including disadvantaged and vulnerable people, and people with low levels of digital literacy. This is frustrated both by the nature of the complex technologies in use, and the fact that they are sourced privately and subject to commercial protection. Even the staff using the tools may not know exactly how they work.

3.6 Moreover, we believe welfare decisions should be human decisions. However, it appears that some decisions are being effectively deferred to automated systems and given merely administrative sign-off by staff. This is, in part, due to ineffective laws.

4. INEFFECTIVE LAWS & THE DIGITAL REVOLUTION

Data Protection Act 2018

4.1 The Data Protection Act 2018 contains broad exemptions for law enforcement purposes, and as such fails to sufficiently protect citizens' rights – including the right to be free from purely automated decisions

4.2 The GDPR safeguards individuals against significant decisions based solely on automated processing.[25] However, the UK's Data Protection Act 2018 makes exemptions from this important GDPR right. Section 14 of the Data Protection Act 2018 permits purely automated decisions with legal or similar significant effects to be made about a subject, in absence of the subject's consent – so long as the subject is notified that the decision was purely automated after the fact. The subject is then to be afforded just one month to request a new decision if they wish.

4.3 However, we are not aware of individuals being notified of purely automated decisions by police, or local authorities, despite the amount of automated processing in use as described above.

4.4 This is likely because under section 14 of the Data Protection Act 2018, automated decisions that have significant legal or similar effects on a subject are not necessarily classified as "purely automated" if a human has administrative input. For example, if a human merely ticks to accept and thus enact a serious automated decision, the decision would not need to be classified as "purely automated" under law and as such, the minimal safeguards of notification and re-evaluation would not even apply.

4.5 Therefore, welfare and justice decisions could be being made that are for all intents and purposes automated decisions, without individuals being notified of this fact or of their right to appeal. We raised concerns about this during the passage of the (then) Data Protection Bill 2018, which were echoed by the Deputy Counsel to the Joint Committee on Human Rights who said, "There may be decisions taken with minimal human input that remain de facto determined by an automated process".[26]

25 GDPR, Article 22

4.6 The Data Protection Act 2018 in fact throws open the door for authorities to make significant decisions about people based on big data and automated processing – and weak legal definitions mean that the few safeguards there are may not even apply.

4.7 **Big Brother Watch believes that two important amendments are required to the Data Protection Act 2018. First, decisions that engage individuals' human rights must never be purely automated decisions; second, automated decisions should be more clearly defined as those lacking *meaningful* human input.**

Digital Economy Act 2017

4.8 Another recent law, the Digital Economy Act 2017 (DEA), undermines privacy in the context of the digital revolution.

4.9 Part 5, Chapter 1 of the DEA permits mass data sharing between public authorities and private companies for the improvement or targeting of a public service or benefit provided to individuals or households. Whilst ensuring access to state benefits is a worthy aim, it must be pursued in a proportionate manner and in accordance with data protection law. Critically, this Act lacks a framework for transparency around the data sharing agreements that are made.

4.10 Government suggested that the DEA would allow authorities to use bulk data to "identify" and intervene in the lives of "troubled families".[27] This arguably amounts to profiling and risks not only breaching Chapter 3 GDPR, but perpetuating discrimination. We were concerned to discover that multiple councils are using bulk data and automated processing to predict which children might join gangs, for example.[28]

4.11 Section 41 DEA further extends the applications of data sharing within and between the state and private companies. Other than fulfilling the purposes for which the data was ostensibly shared, information can be used to prevent or detect crime or anti-social behaviour, for criminal investigations, for legal proceedings, for "safeguarding vulnerable adults and children", for HMRC purposes, or as required by EU obligations. This is a very enabling law that could further institutionalise big data in modern governance and administration. However, the systemic lack of transparency of such data sharing agreements means we know little about how this is working in practice and how people's privacy is being affected.

---

26 Note from Deputy Counsel, 'The Human Rights Implications of the Data Protection Bill', 6 December 2017 (https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf)

27 Digital Economy Bill Factsheet: Better Public Services, Department of Culture, Media and Sport

28 https://www.theguardian.com/society/2018/sep/17/data-on-thousands-of-children-used-to-predict-risk-of-gang-exploitation

4.12 Big Brother Watch recommends that a public inventory of public-private information sharing agreements is established.

5. PRIVACY, RIGHTS & ONLINE REGULATION

5.1 We wish to briefly address forthcoming regulation and possibly legislation regarding internet intermediaries and 'online harms'. The Government's Online Harms white paper is yet to be published, but we would welcome an opportunity to make further submissions to the Committee about online regulation when it has been published, as this will set the tone for some of the most significant government regulation of online spaces in recent years.

5.2 Online regulation will influence the norms for new modes of social interaction; inscribe limitations on people's freedom; balance power relationships between businesses, citizens and the state; and effectively write lasting rules into a changing world.

5.3 We believe that content regulation should be based on human rights and a rule of law model, centring transparency, foreseeability, equal and consistent application of the rules, and procedural fairness. Government should encourage internet intermediaries to respect human rights and the rule of law model, but instead seems intent on taking a more interventionist role in specific policies (including subjective notions of 'harm').

5.4 Whilst we look to government for positive influences and regulation where necessary, internet intermediaries inevitably have an important role to play in upholding human rights in the modern content. Internet platforms wield great power over society and politics. Their architecture and algorithms shape the information we receive, and the information we are permitted to share. They rank and order information according to criteria we generally can't see, change or challenge. They moderate speech, and permit and restrict digital existence in vast public spaces. With millions and even billions of users, some of these platforms perform as public utilities. In that light, their role and responsibility to uphold basic rights should be clear.

5.5 Currently, relationships between users and platforms are constructed through contract law. Far from serving to protect the rights of users, terms are constructed to protect the commercial interests of the platforms. It is a considerable challenge to move multi-billion dollar platforms from a model where commercial interests are centred to one where their users' interests and wider society is centred.

5.6 There is an evolving acknowledgement of the role businesses should play in protecting human rights. In 2008, the UN Human Rights Council approved a framework for business and human rights, whereby States are the primary duty bearers in securing the protection of human rights, corporations have the responsibility to respect human rights - and both entities are joint duty holders in providing effective remedies against rights violations.

5.7 In 2015, the Internet Governance Forum (IGF) delivered recommendations on Terms of Service and Human Rights, focusing on three components: privacy, freedom of expression and due process. The IGF said that *"certain platforms should be seen more as "public spaces"* that *"increasingly play an essential role of speech enablers".* This is clearly the case, and those platforms have an unprecedented ability to exclude citizens' digitally and effectively deny modern public rights of access in the digital world.

5.8 It is paramount that freedom of expression on online platforms is protected just as it is in the public square. For that reason, we believe that major platforms should not censor content beyond the extent to which it would be censored under human rights law. This position was also promoted by the IGF. Achieving this requires positive government influence, and unavoidably requires voluntary action from internet intermediaries.

5.9 Furthermore, platforms should model their enforcement approach on rule of law principles which provide for a robust governance framework, suitable for an actor that negotiates the rights of citizens. Transparency, foreseeability, equal and consistent application of the rules, and procedural fairness, are key safeguards for citizens online. Currently, the terms of service model effectively gives most platforms absolute power and complete discretion as to their application of it. Rule of law principles would moderate that power to ensure its exercise is limited, fair and forseeable.

5.10 Finally, we believe the single most important regulatory action government could take would be to ban micro-targeted online advertising in the UK. This would not only deter intrusive tracking of citizens online and privacy breaches, but would protect citizens from personalised advertising that risks exploiting and manipulating them whilst sowing divisiveness – and, in extremis, even manipulating elections and political swings.

5.11 Big Brother Watch recommends that micro-targeted online advertising is banned in the UK.

Silkie Carlo

Griff Ferris