BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Big Brother Watch's response to the Online Harms White Paper Consultation

July 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.

Contact

Silkie Carlo

Director, Big Brother Watch

Email: silkie.carlo@bigbrotherwatch.org.uk

Direct line: 020 8075 8478 | Media line: 07730 439257

Contents

INTRODUCTION

The internet is a global communications network that has revolutionised the modern world and become an essential pillar of public infrastructure. To regulate the internet is to regulate the modern space we spend most of our lives connected to. It is the environment in which we access news and information, develop our personalities, find employment, create businesses, build social lives, maintain family relationships, shop and access services, engage in political campaigns and express ourselves.

The internet is a critical utility – and our day to day experience of it is increasingly mediated by internet intermediaries that wield huge power. Facebook, for example, has a larger user base than the population of any country in the world,[1] a greater GDP than many nation states,[2] and has just launched its own currency.[3] Social media platforms are our modern public squares – and increasingly, our modern high streets, meeting rooms and town halls. It can be argued that social media companies and the information they filter to us are gradually creating the lenses through which we see the world.

Clearly, we cannot allow the world and our rights within it to be reshaped according to the profit-driven whims of Silicon Valley's tech elite.

However, any Government influence must be proportionate, limited, and in the interests of the people. Government's role should be focused on upholding the rule of law online and protecting its citizens' rights – not eroding them. We agree with Government that rules that apply in the offline world should apply in the online world – but we do not agree that rules that do not apply in the offline world should be imposed on the online world. However, the Online Harms White Paper proposes the expansion of restrictions on freedom of expression and intrusions on privacy and that would never be possible or permissible in the offline world. The plans go far beyond upholding the rule of law online and are in fact focused on censoring and demoting lawful expression that could be deemed "harmful" – a term left undefined.

---

[1] Facebook has 2.38 billion monthly active users as of March 31, 2019 (https://newsroom.fb.com/company-info/). China's population is 1.4 billion. Facebook's annual turnover

[2] 25 giant companies that are bigger than entire countries – F. Belinchon and R. Moynihan, Business Insider, 25 July 2018 (https://www.businessinsider.com/25-giant-companies-that-earn-more-than-entire-countries-2018-7?r=US&IR=T)

[3] Facebook announced the launch of Libra in June 2019

The legal framework around communications offences is already expansive

This is not only draconian - it is unnecessary. The UK already has expansive laws governing speech-related offences that can be used to prosecute violent, hateful and harmful forms of speech and behaviour online. This includes laws prohibiting speech that causes harassment, alarm, distress, or fear (Protection from Harassment Act 1997; Public Order Act 1986); speech that is deemed grossly offensive and purposefully annoying or distressing (Malicious Communications Act 1988; Communications Act 2003); and speech that incites hatred on the basis of race, religion or sexual orientation (Crime and Disorder Act 1998; Race and Religious Hatred Act 2006).

The Law Commission's recent scoping report on abusive and offensive online communications found that, whilst some clarifications and reforms may be useful, the legal framework around communications offences is already expansive:

> *The broad terms used in the* (existing) *offences also means that they are generally flexible enough to cover the huge variety of offensive and abusive online communications, and provide scope to adapt to future developments.*[4]

This report is acknowledged in the Online Harms White Paper:

> *(…) the Law Commission concluded that behaviour is broadly criminalised to the same extent online as offline* [5]

This means that law enforcement agencies could use existing laws to deal with many of the harms people might experience online.

However, Government is seeking to deputise enforcement to internet intermediaries, imposing an open-ended "duty of care" on them to protect users not only from unlawful content but from 'harm'. The proposals would see companies tasked with policing the speech of millions, far beyond existing legal boundaries, leading to a wave of privatised monitoring and censorship.

[4] Summary of Scoping Report: Abusive and Offensive Online Communications – Law Commission, 1 November 2018, p.5
[5] Online Harms White Paper – DCMS and The Home Office, April 2019, p.34

The proposals conflict with fundamental rights principles

International human rights covenants to which the UK is a signatory, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Charter of Human Rights; and the UK's Human Rights Act 1998, impose a duty on the UK to ensure an enabling environment for, and to protect, people's right to freedom of expression and information and their right to privacy. The proposals in this White Paper conflict with those obligations.

The proposals would not only erode our rights. It would undermine the role law enforcement needs to play online and instead reposition social media companies, which are already incredibly powerful, as privatised enforcement agencies. Citizens, whose data has been used, abused and sold by these companies to their disadvantage, are expected to trust this model. The reality is that the Government's over-bearing and ill-defined approach would result in the state-sanctioned monitoring and censorship of lawful expression online on a scale never before seen in a democracy.

We must be mindful of how the policy proposals in the Online Harms White Paper could be used by less democratic governments. To focus an enforcement framework that would affect vast swathes of modern communications on the undefined notion of "harm" would be to open the door to subjective and politicised censorship. Our Government has been clear that it is "leading international efforts" for the online harms approach to be a blueprint for international regulation, building "a global coalition of countries all taking co-ordinated steps".[6] However, if the proposals in the Online Harms White Paper were exported internationally, it would be a disaster for human rights and freedom of speech not only in the UK but overseas.

[6] Online Harms White Paper – DCMS and The Home Office, April 2019, p.6

RECOMMENDATIONS

- **The policy requires a root and branch rethink.** The Online Harms White Paper is based on a fatally flawed and fundamentally inappropriate model, imposing a "duty of care" and policing subjective "harm". This would create a two-tier system where the right to free speech is more limited online than offline, eroding the right to freedom of expression.

- **Government should work with major platforms that act as our digital public squares to develop digital constitutionalism.** Government should encourage the platforms to model their rules on human rights and domestic law, and to reflect rule of law principles such as transparency of rules, foreseeability of their application, fairness of processes, the right to appeal, and equal and consistent application of the rules.

- **The rule of law must be upheld online.** Rules that apply in the offline world must apply in the online world, yet the White Paper lacks proposals about the role of law enforcement. Rules that do not apply in the offline world should not be imposed on the online world.

UK Government should be taking leadership in protecting and promoting rights whilst upholding the rule of law online – not eroding them. This would set a world-leading, democratic example to countries around the world.

Our Government should use its influence to promote human rights norms and the rule of law as an enforcement model for major digital platforms. This means guiding companies in helping to protect our rights to freedom of expression and privacy, and promoting enforcement that centres transparency, foreseeability, fairness, and equal and consistent application of the rules. It also means law enforcement and social media companies working to make sure the law is upheld online. Neither a new regulator, nor social media companies, should censor lawful content.

This approach would ensure that harms online are drastically reduced whilst creating free and democratic digital public squares built to last.

THE ONLINE HARMS WHITE PAPER

The 'Online Harms White Paper' developed by the Department for Digital, Media, Culture and Sport (DCMS) and the Home Office was published in April 2019, setting out proposals to regulate user content across the entire internet. The regulation centres on imposing a "duty of care" on all companies that facilitate people to interact with others online, to protect them from "harm". Government aims to export this as an international regulatory model.

Firstly, we believe the "harms" approach and "duty of care" obligations that underpin the policy proposals are fundamentally flawed and destined to negatively impact the health of fundamental rights to privacy and freedom of expression in the UK. As such, this policy approach is wrong and the White Paper requires a fundamental rethink. In our response to this consultation, we explore the multitude of serious issues the "harms model" would give rise to.

A "duty of care" is inappropriate for internet intermediaries

The "duty of care" approach is inappropriate for internet intermediaries and other companies online that facilitate people to interact with one another. It effectively makes companies responsible for how third parties (members of the public) behave towards one another, and puts them in the business of policing people's conversations. To hold companies responsible for the actions of individuals online is to misdiagnose the problem and misplace the responsibility.

It is unprecedented for a private company to be under a duty of care to prevent harm resulting from the conduct of others.[7] A duty of care ordinarily refers to a company's duty to ensure its own risk-creating actions do not cause physical injury to others (for example, a stockroom manager has a duty to ensure employees use safe lifting equipment to avoid physical harm). Clearly, these conditions do not apply to internet intermediaries – to provide platforms for people to interact is not a risk-creating action, and there is no risk of physical harm.

Legal experts have remarked on the "radical departure" from precedents on duties of care in this White Paper:

[7] See also, UK Supreme Court, *Robinson v Chief Constable of West Yorkshire Police,* 2018

> *The limits on duties of care exist for policy reasons that have been explored, debated and developed over many years. Those reasons have not evaporated in a puff of ones and zeros simply because we are discussing the internet and social media. The government's proposed online duty of care would disregard these and other limits, but the White Paper does not acknowledge its radical departure from existing principles.*[8]

Government may intend to radically reinvent the concept of a "duty of care", but this should not be proposed without serious consideration for the impact that such an expansion of the concept would have on the legal landscape. To apportion generic liability and a psychological duty of care to companies over interactions between members of the public could easily make for a very different society to the one we currently live in.

The regulator should not seek to enforce companies' terms and conditions

One of the ways the proposed government-appointed regulator would ensure companies are fulfilling their duty of care is by ensuring companies are upholding their own terms and conditions:

> *The regulator will assess whether companies have fulfilled their duty of care, including by reference to relevant codes of practice,* ***and compliance with the company's own relevant terms and conditions****. Failure to meet these obligations may result in enforcement action by the regulator.*[9]

Whilst companies sticking by their terms and conditions can be seen as a good in and of itself, it is widely recognised that the online data trade means many online companies' terms and conditions are designed for their own economic benefit and legal protection rather than to prioritise the interests of their users. The terms of service model regulating the relationship between platform and user effectively gives many platforms absolute power and complete discretion as to their application of it.[10] And it would be a difficult position for a regulator to cherry-pick which areas of a company's terms and conditions to assess for "harm". As such, it would seem a controversial position for a Government-appointed regulator to oversee private companies in

---

[8] *Online Harms White Paper – Response to Consultation,* by Graham Smith, 28 June 2019, para. 1.7, p.3: https://drive.google.com/file/d/1zULZ8hvXqoMQ1UguCPx01RYNqjhWbTt2/view
[9] Online Harms White Paper – DCMS and The Home Office, April 2019, p.43 – emphasis added
[10] For further analysis, see *Digital Constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms* – N. Suzor, July 2018, in Social Media + Society

effectively upholding those terms and conditions – sets of rules that are not neutral, and which have complex implications.

Ensuring companies comply with their terms and conditions raises particularly significant issues where those terms apply to speech issues. Platforms' rules (if not always their enforcement) typically go much further than domestic laws in limiting speech. For example, Facebook's community standards include policies on 'objectionable content' that go far beyond the limits set in domestic law. It would be distinctly wrong for a regulator to oversee the fulfilment of terms and conditions that enforce censorship of lawful speech. For the regulator to adhere to and endorse speech standards set in private 'community standards' would show a worrying lack of commitment for this country's laws and case law on free speech that have evolved over many years. Such proposals would make the government-appointed regulator complicit in limitations on free speech.

Recognising major platforms as the public's modern public squares, Government would do better to play a role building digital constitutionalism into the tech giants' terms and conditions, embedding human rights and rule of law principles as a basic standard. Government should be using its power and influence to encourage companies to reflect the standards set in UK law, above all human rights law – not to adhere to the standards set in their own self-interested terms and conditions.

The rule of law must be upheld online

We believe that the rule of law must be upheld online. Some of the proposals in the White Paper are aimed towards this, such as the suggestion of codes of practice for companies, drawn up by a regulator and law enforcement, on tackling the sale of illegal goods and other illegal harms. The codes of practice would "establish requirements and processes, where appropriate and proportionate, for referring illegal content and activities to law enforcement".[11]

However, of the seven main activities expected of the companies under the proposed "duty of care", supporting law enforcement investigations is just one.[12] The proposals are mainly focused on "tackling harm" – a broad and nebulous concept that far from upholding the rule of law online would in fact erode free expression.

[11] Online Harms White Paper – DCMS and The Home Office, April 2019, para. 6.7, p.61
[12] Online Harms White Paper – DCMS and The Home Office, April 2019, para. 7.4, p. 64

The proposals would erode lawful expression online

The Government's proposals extend beyond seeking to prevent and prosecute crime and in fact compel companies to prevent "legal harms"[13] online. The White Paper proposes targeting undefined "unacceptable content and activity"[14] on the basis that "beyond illegal activity, other behaviour online also causes harm".[15] The regulator is also expected to issue codes of practice to companies specifically about content that is "not necessarily illegal" but that may "directly or indirectly" cause "harm" to other users.[16] This means that an unelected regulator will be tasked with narrowing what constitutes free speech in the digital environment.

This is a dangerous approach.

Lawful expression must not be subject to state-sponsored censorship. Any extensions to the limitation on citizens' right to freely express themselves must be decided by parliament, exercised through statute law, and meet human rights standards. Freedom of expression is protected by multiple human rights frameworks to which the UK is a signatory, notably the European Convention on Human Rights (ECHR). The ECHR is clear that any restrictions on free expression must be prescribed by law and necessary in a democratic society. However, the restrictions on free expression that this White Paper proposes would be prescribed by a regulator, not by law or parliament. The proposal for an unelected, state-appointed regulator to interfere with lawful expression through pressure on private companies is distinctly undemocratic and inherently rights-abusive.

"Harms" are not defined

The Online Harms White Paper provides an initial list of the types of harmful content that would be targeted but notes that the list is "neither exhaustive nor fixed" to enable the regulator to take "swift regulatory action to address new forms of online harm".[17] "Harm" is not a defined concept in the paper, and some of the harms that are presented lack a robust evidence base.[18] It is difficult to conceive of a lower threshold for regulatory action than the undefined and inherently subjective notion of speech-related

[13] Online Harms White Paper – DCMS and The Home Office, April 2019, para 2.8, p.34
[14] Online Harms White Paper – DCMS and The Home Office, April 2019, p.5
[15] Online Harms White Paper – DCMS and The Home Office, April 2019, p.16
[16] Online Harms White Paper – DCMS and The Home Office, April 2019, p.68
[17] Online Harms White Paper – DCMS and The Home Office, April 2019, para. 2.2, p.30
[18] This view is shared by Dr Vic Baines. See *On Online Harms and Folk Devils: Careful Now* by Dr. Vic Baines, Medium, 24th June 2019: https://medium.com/@vicbaines/on-online-harms-and-folk-devils-careful-now-f8b63ee25584

"harm", which differs from person to person. Such an elusive threshold presents serious risks to freedom of speech.

The proposals would act as a blank cheque for the regulator to enforce the censorship, control or demotion of any category of lawful content, redefining the practical limitations on people's free expression online. The right to freedom of expression has long been a closely guarded human right, protected in law, with any restrictions subject to the democratic parliamentary process. However, the power exercised by the online regulator would bypass this vital democratic process, creating a two-tier system whereby the increasingly ubiquitous online tier would be, for all intents and purposes, untethered from decades of existing law and highly susceptible to political swings of the day. This situation is precisely what Government should be seeking to change – not endorse.

The initial harms list provided is divided into three categories: "Harms with a clear definition", "Harms with a less clear definition", and "Underage exposure to legal content".[19]

The first category consists of issues covered by the law (e.g. harassment, sale of dugs, modern slavery) and as such represents areas that naturally invite law enforcement intervention, intermediary co-operation, and need not be contextualised in this extra-judicial "harms" model.

The second category is deeply problematic and refers to generalised types of content. The items listed include "disinformation", "trolling", "extremist content and activity" and "intimidation".

It is wrong to conflate a policy approach to dealing with unlawful activity online with policy dealing with lawful activity simply because it might be deemed 'harmful'. As one online law enforcement expert put it, by the very act of including both lawful and unlawful categories in the white paper "*the authors suggest they are in some way comparable and that they allow for a similar level of debate on their acceptability. They are not and they do not.*"[20]

[19] Online Harms White Paper – DCMS and The Home Office, April 2019, p.31

[20] *On Online Harms and Folk Devils: Careful Now* by Dr. Vic Baines, Medium, 24th June 2019: https://medium.com/@vicbaines/on-online-harms-and-folk-devils-careful-now-f8b63ee25584

Disinformation

Terms such as "disinformation" can be subjective and easily politicised. Under this banner, the White Paper proposes imposing a duty on companies to "help users understand the nature and reliability of the information they are receiving", to "minimise the spread of misleading and harmful disinformation" and to "(promote) authoritative news sources".[21] It is important to remember that these regulations could be imposed, without clear legal definitions, not only on organisations but on members of the public sharing and accessing information online.

Some legitimate activities, such as publishing the source of information or a social media page, including the country of origin (a practice recently adopted by Facebook, though apparently not in a consistent or apolitical way[22]), could fall under the category of helping users "understand the nature" of the information they access.

However, it should generally not be the place of a private company to assess and then instruct their users as to the "reliability" of the information and news sources they access. This is a highly subjective task best fulfilled by internet users themselves, who can optionally conduct wider research or access fact-checking websites online. This is much easier online than it is in a library and offline public spaces. The critical faculties of members of the public are not the responsibility of tech companies. Nor are tech companies best placed to judge the "reliability" of information.

The obligation to promote "authoritative" news sources is highly subjective and easily politicised. A democratising effect of the internet has been the opening of spaces for marginalised voices, blogs, campaign journalism and more disintermediated news sharing. Citizen journalism online has made a significant contribution to media as a whole, offering new and diverse perspectives, rapid story-telling, inclusive media and audience participation. Citizen journalism has played a major role in 21st Century political events,[23] including the Occupy movement and the Arab Spring, and this has relied on the more equal playing field online for individuals to gain exposure and generate revenue. If government enforces this "authoritative" curation role on internet platforms, the space for participatory media that has enriched society over the past decade will shrink and news mediation will be more likely to remain monopolised.

---

[21] Online Harms White Paper – DCMS and The Home Office, April 2019, p.71
[22] *Facebook Suspends Three Pages With Millions of Video Views, Saying They Need to Disclose Russia Ties* – Tom McKay, Gizmodo, 16th February 2019: https://gizmodo.com/facebook-suspends-three-pages-with-millions-of-video-vi-1832679030
[23] https://www.britannica.com/topic/citizen-journalism

Intimidation

Non-criminal "intimidation" is also listed as a harm, but lacks definition. Intimidation is specifically referred to in the White Paper in relation to "online abuse of public figures".[24] However, given the remarkable breadth of the UK's existing laws on speech and communication crimes, there are clear risks to intervention in lawful speech to public figures that could threaten political expression and limit democratic participation.[25] It is easy to see how political pressure on the regulator could lead to lawful, albeit unsophisticated or ill-mannered, expression towards politicians and other public figures being suppressed. Such an intervention could unduly limit people's rights and undermine democracy.

Interfering with legal "harms" not only encroaches free expression – it may be counter-productive

Self-harm

Much of the impetus for the Government's "online harms" proposals came from increasing media concern about content relating to self-harm and suicide online. Recent months have seen emotive news headlines that have not necessarily been evidenced (for example, "Instagram 'helped kill my daughter'", BBC, Jan 2019)[26] and there has been an atmosphere of growing panic on this issue.

As Dr Vic Baines (a former law enforcement intelligence analyst, EMEA Trust & Safety Manager at Facebook and now Visiting Associate at the Oxford Internet Institute) put it:

> *(…) the implication that tech firms bear sole responsibility for online safety issues has taken root. The dominant political and mainstream media tactic appears to be to lay these problems squarely at the doors of the companies—ignoring the important roles to be played by central government, law enforcement, local authorities, educators, civil society groups, parents and carers (the list goes on) (…) it cannot be the responsibility solely of tech*

[24] Online Harms White Paper – DCMS and The Home Office, April 2019, p.24
[25] See also Written evidence from Index on Censorship (DFF0015) to the Joint Committee on Human Rights' "Democracy, free speech and freedom of association" inquiry, 22 March 2019: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/democracy-free-speech-and-freedom-of-association/written/98529.html
[26] "Instagram 'helped kill my daughter'" - BBC, 22nd January 2019: https://www.bbc.co.uk/news/av/uk-46966009/instagram-helped-kill-my-daughter

> *companies to provide solutions to the woeful under-resourcing of mental health provision for young people (…)*[27]

There is no question that content encouraging or assisting suicide should be removed – encouraging and assisting suicide is an offence,[28] which the CPS is clear applies equally to content online.[29]

It is important to have a clear understanding of the scale of this problem. The White Paper reports a finding from a recent study that 70% of young people who harmed with suicidal intent and 22.5% of young people as a whole "reported self-harm and suicide-related internet use", and reports that this is a "threat".[30] However, this overlooks some key facts from the study. The study found that 3.1% of young people reported exposure to information on how to hurt or kill yourself – the larger statistics include young people who have simply come across news reports online about people who have hurt or killed themselves or who had seen general information about the topic.[31] Therefore, exposure to unlawful and harmful content is much smaller than perhaps suggested.

The White Paper also cites the study as having found that 8.2% of young people actively searched for information about self-harm and similarly reports this is a "threat".[32] However, this overlooks the study's finding that most of this activity was in fact "reassuring": a larger proportion of young people accessed sites offering help, advice and support (8.2%) than sites offering information on how to hurt or kill yourself (3.1%), and most people who had accessed potentially harmful sites had also accessed help sites (81%).[33]

Analysing the White Paper, Dr. Vic Baines wrote:

> *As a former government threat analyst, I can't help but be concerned when I see glaring gaps in evidence, misinterpretation and misrepresentation of data,*

---

[27] *On Online Harms and Folk Devils: Careful Now* by Dr. Vic Baines, Medium, 24th June 2019: https://medium.com/@vicbaines/on-online-harms-and-folk-devils-careful-now-f8b63ee25584
[28] Suicide Act 1961, s.2
[29] Suicide: Policy for Prosecutions in Respect of Cases of Encouraging or Assisting Suicide, see para.20 p.5, para. 25 p.4, para. 43(11) p.6, – Director of Public Prosecutions, October 2014:
[30] Online Harms White Paper – DCMS and The Home Office, April 2019, Box 9, p.19
[31] Mars, B et al. (2015). Exposure to, and searching for, information about suicide and self-harm on the internet: Prevalence and predictors in a population based cohort of young adults' Journal of affective disorders, 185, 239-45. Available at: https://doi.org/10.1016/j.jad.2015.06.001
[32] Online Harms White Paper – DCMS and The Home Office, April 2019, Box 9, p.19
[33] Mars, B et al. (2015). Exposure to, and searching for, information about suicide and self-harm on the internet: Prevalence and predictors in a population based cohort of young adults' Journal of affective disorders, 185, 239-45. Available at: https://doi.org/10.1016/j.jad.2015.06.001

generalisations from specific cases (…) and emotional language on subjects about which we absolutely need to be as objective as is humanly possible.[34]

Whilst the White Paper rightly acknowledges, "users should be able to talk online about sensitive topics such as suicide and self-harm"[35] the proposals would appear to interfere with their right to privately and freely do so in practice. The White Paper suggests the regulator ensures companies are "blocking users responsible for activity which violates terms and conditions"[36] – not the law - meaning a state-appointed regulator could endorse the silencing of vulnerable people's lawful expression. This could have serious impacts on people's rights and mental health.

The White Paper also proposes that companies intervene with "vulnerable users" and those "who actively search for or have been exposed to (suicidal and self-harm) content".[37] Whilst well-intended, this could easily result in an over-reach and justify mass monitoring and data-gathering practices that could have negative consequences and undermine users' privacy. Many people, whether suffering mental ill health or not, will feel anxious about a for-profit, data exploitation company like Facebook analysing, collecting data on, and intervening in their mental health. It is concerning that Government is encouraging such a role for these internet companies.

There is already a predictive element to this too, raising novel legal and ethical questions about how such a duty of care will operate with the technologies of the near-future. For example, Facebook has started using artificial intelligence (AI) and predictive analytics to identify users deemed at risk of suicide, in order to launch interventions.[38] It has been claimed that some AI software is now able to predict suicide attempts two years in advance.[39] Many people would be deeply uncomfortable being subject to such intrusive analysis, and indeed, their legal rights would be engaged.
It is natural that people experiencing self-harm or suicidal thoughts will use the internet as a resource – it does not mean that such internet use is encouraging, increasing or causing harmful behaviours and the research does not identify such a causal relationship. Government should not make policy, much less export policy internationally, that is built on the misconception that exposure to mental illness is

[34] *On Online Harms and Folk Devils: Careful Now* by Dr. Vic Baines, Medium, 24th June 2019: https://medium.com/@vicbaines/on-online-harms-and-folk-devils-careful-now-f8b63ee25584
[35] Online Harms White Paper – DCMS and The Home Office, April 2019, p.72
[36] Online Harms White Paper – DCMS and The Home Office, April 2019, p.73
[37] Online Harms White Paper – DCMS and The Home Office, April 2019, p.72
[38] *Facebook Using Artificial Intelligence to Help Suicidal Users* – Aatif Sulleyman, The Independent, 2 March 2017.
[39] *Artificial Intelligence Can Now Accurately Predict Suicide Attempts Two Years in Advance* – Paul Tamburro, Crave, 3 March 2017

contagious. A shrinking private sphere may deter people from seeking social support and a safe space to freely express themselves. It is important that the internet remains a rich resource for people to openly explore mental health issues, with their rights to privately and freely access information protected.

Lawful content would be policed in algorithms and recommendation systems

The White Paper's proposals would unduly limit free expression not only through the regulation of content but the regulation of recommendation systems that influence what information is promoted and exposed online. Government wants companies to take "reasonable steps to take to ensure that users will not receive recommendations to hateful or inappropriate content"[40] but does not define what is meant by "inappropriate".

The proposals include making companies change their algorithms to stop the promotion of self-harm related content.[41] Whilst a well-intended aim, government forcing private companies to control the visibility of categories of lawful information is a slippery slope. Once one type of lawful content is removed from recommendation systems, it will be inevitable that many further types of lawful content will also be removed. There are clear risks to giving a Government-appointed regulator such power over digital information flows.

Our view is that if content should not be online (i.e. it is unlawful) it should be removed, not technologically siloed.

Technological enforcement will erode due process

The Government puts great emphasis in the White Paper on the use of technological tools, including AI, to enforce content regulations online. It proposes that the regulator has "a legal obligation to support innovation" and even suggests creating "machine executable regulation.[42] The Government also proposes its own direct involvement, committing to "work further with research organisations to understand how AI can best be used to detect, measure and counter online harms".[43]

---

[40]Online Harms White Paper – DCMS and The Home Office, April 2019, p.69
[41]Online Harms White Paper – DCMS and The Home Office, April 2019, p.73
[42]Online Harms White Paper – DCMS and The Home Office, April 2019, p.56
[43] Online Harms White Paper – DCMS and The Home Office, April 2019, p.80

AI for speech regulation is a very blunt tool. It is rarely best placed in content moderation, which deals with nuanced areas of speech, law and the adjudication of citizens' rights. Whilst automation can play a role in detecting extremely serious illegal material such as child abuse imagery at scale, the White Paper describes building a role for AI in analysing and countering "hate speech" and "to detect and address harmful and undesirable content".[44] Neither "harmful" nor "undesirable" are defined. Government policy to use AI to automatically detect "undesirable" speech in the public domain is a chilling and fundamentally authoritarian notion.

The White Paper makes positive reference to Google's Perspective API – a machine-learning tool that scores the "perceived impact a comment might have on a conversation".[45] Administrators of comment sections (including Disqus, New York Times, El Pais) use Google's API to flag potentially harmful or 'toxic' content to moderators. However, it is a crude tool that flags words such as "stupid", "rubbish" and even "racist" as the highest levels of toxicity. It flags the phrase "I'm angry about women being raped" as the highest level of toxicity, but the phrase "I'm angry at women" is not flagged at all.[46] It is concerning that the White Paper makes reference to this crude tool without identifying its serious, quite fundamental short-comings. Policy making in this area should be evidence-led – not led by blind faith in technology to make complex adjudications about semantics, rights and legal boundaries.

The White Paper also suggests "AI can be beneficial in the automatic detection of content, or automatically fact-checking articles."[47] Such technologies are at best experimental, and are simply unable to deal with the delicate nuances involved with fact-checking news. Moreover, the very premise of the state endorsing such tools to automatically judge the veracity of news is troubling and could easily conflict with principles of a free press and due process.

Automation has a limited role – for example, detecting image hashes to identify child sex abuse imagery at scale. However, there is no place for automated mass monitoring of speech online, nor in complex and nuanced determinations of the legality, much less acceptability, of people's speech online.

[44] Online Harms White Paper – DCMS and The Home Office, April 2019, p.80
[45] https://perspectiveapi.com
[46] Our own testing, last checked 28 June 2019 on Google's Perspective API: https://perspectiveapi.com
[47] Online Harms White Paper – DCMS and The Home Office, April 2019, p.23

Harsh punishments will encourage companies' zealous censorship

The White Paper proposes unprecedented punishments for internet companies in the UK and overseas, and even for individual staff members, should they be found to "fail to fulfil their duty of care".[48] The range of repercussions is severe, and there is an emphasis on the speed of compliance to avoid incurring them: the regulator would "incentivise companies to fulfil their obligations quickly".[49] It is unprecedented for the Government to seek to punish technology companies for essentially failing to act as effective law enforcement auxiliaries and even for failing to censor or demote lawful content. If these proposals go ahead, there will be a distinct chilling effect that will motivate companies to monitor, demote and censor expression very keenly.

Such a chilling effect has been seen in Germany, since the Network Enforcement Act 2017 ('NetzDG') was passed. We were concerned to see reference made to NetzDG in the White Paper, without acknowledging the serious impact it has had on rights. The Act threatens fines of up to €50 million for social media companies that fail to remove illegal content within 24 hours. It is extremely heavy-handed and the imposed threat of such a large fine incentivises profit-driven social media companies to err on the side of caution and over-censor content. Human Rights Watch has called on German lawmakers to "promptly reverse" NetzDG and explained that it is "vague, overbroad, and turns private companies into overzealous censors to avoid steep fines, leaving users with no judicial oversight or right to appeal."[50] Article 19 warned that "the Act will severely undermine freedom of expression in Germany, and is already setting a dangerous example to other countries that more vigorously apply criminal provisions to quash dissent and criticism, including against journalists and human rights defenders."[51] The UN Special Rapporteur on Freedom of Expression, David Kaye, warned that NetzDG "raises serious concerns about freedom of expression and the right to privacy online", and argued that "censorship measures should not be delegated to private entities."[52] The law has also been criticised by the German broadcast media for

[48] Online Harms White Paper – DCMS and The Home Office, April 2019, p.59
[49] Online Harms White Paper – DCMS and The Home Office, April 2019, p.59
[50] Germany: Flawed Social Media Law – Human Rights Watch, 14 Feb 2018: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law
[51] Germany: Act to Improve Enforcement of the Law on Social Networks undermines free expression - Article 19, 1 Sept 2017: https://www.article19.org/resources/germany-act-to-improve-enforcement-of-the-law-on-social-networks- undermines-free-expression/
[52] Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 1 June 2017: https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf

turning controversial and censored voices into "opinion martyrs".[53] None of these facts were acknowledged in the White Paper.

In the Online Harms White Paper, the various ways the regulator is proposed to enforce the duty of care would include "publishing public notices", "issuing civil fines", and "measures to impose liability on individual members of senior management" – even criminal liability.[54] [55] Furthermore, the White Paper proposes that the regulator should be empowered to "disrupt the business activities of a non-compliant company",[56] which would even include powers "to force third party companies to withdraw any service they provide that directly or indirectly facilitates access to the services of the first company, such as search results, app stores, or links on social media posts".[57] In addition, it is proposed that the regulator is empowered to force Internet Service Providers (ISPs) to block non-compliant websites as a "last resort". This would apply to websites that have failed to meet the "outcome requirements for illegal harms" and the decision would be "for the independent regulator alone".[58] The proposal for search engine, intermediary and ISP blocking is severe; the proposal to base such blocks on "outcome requirements" is seriously misguided; and the proposal for these decisions, with profound impacts on rights, to be non-judicial is alarming.

These are extremely serious sanctions with wide-ranging effects, including on third parties such as search engines and ISPs and the public more widely. The idea of the British government appointing a regulator to enforce Chinese-style ISP blocks and search-engine controls over information is extraordinary. Such severe sanctions should not be casually proposed, with such little justification, in a White Paper dealing with both lawful and unlawful content.

This wide range of punishments includes economically and reputationally damaging effects, that would incentivise intermediaries to strictly implement the "duty of care" zealously. That is clearly the Government's intention. But this would also mean closer monitoring of users, more intense policing of speech, and a distinct preference for bad decisions to demote and censor speech over bad decisions to allow speech.

---

[53] https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in- spotlight
[54] Online Harms White Paper – DCMS and The Home Office, April 2019, p.59
[55] https://homeofficemedia.blog.gov.uk/2019/04/08/online-harms-white-paper-factsheet/
[56] Online Harms White Paper – DCMS and The Home Office, April 2019, p.59
[57] Online Harms White Paper – DCMS and The Home Office, April 2019, p.60
[58] Online Harms White Paper – DCMS and The Home Office, April 2019, p.60

The importance of the right to appeal

We welcome the White Paper's proposals to encourage companies to provide "effective and easy-to-access user complaints functions."[59] This is an important safeguard in any process adjudicating over individuals' ability to freely express themselves.

Under the proposals, companies would need to "respond to users' complaints within an appropriate timeframe" and to "take action consistent with the expectations set out in the regulatory framework."[60] This is a very welcome initiative – but the impact relies entirely on the appropriateness of the platforms' rules in the first place. As described above, their current rules limit expression beyond the boundaries set in domestic law, and the proposals in this paper would seek to extend these limitations further still. If the platforms' rules do not uphold people's right to free expression, the benefits of the right to appeal will be limited.

Protecting free expression is not a legal duty of the regulator

The regulator would have a "legal obligation to support innovation" but no such *legal* obligation to ensure people's rights are protected online. Indeed, any such obligation would fundamentally conflict with the proposals, which seek to extend limitations on free expression beyond current law.

The White Paper makes brief references to free expression – but making rhetorical reference to rights does nothing to actually protect them. The Ministers' foreword claims, "The UK is committed to a free, open and secure internet, and will continue to protect freedom of expression online"[61] but there are no policy proposals in the White Paper about how this would be done. Of over 100 pages, there is just one brief section on "Protecting users' rights online", consisting of only three sentences.

This short section says the regulator would have an "obligation to protect users' rights online", though this is not posited as a legal obligation, nor supported by substantive proposals, and as explained above, fundamentally conflicts with the raft of policy proposals in the paper which redraw and restrict users' rights online. This section only says that the regulator would:

[59] Online Harms White Paper – DCMS and The Home Office, April 2019, p.8
[60] Online Harms White Paper – DCMS and The Home Office, April 2019, p.42
[61] Online Harms White Paper – DCMS and The Home Office, April 2019, p.3

> *ensure that the new regulatory requirements do not lead to a disproportionately risk averse response from companies that unduly limits freedom of expression.*[62]

This fails in a number of respects. Firstly, there are no substantive policy proposals as to how the regulator would measure or protect freedom of expression online, but plenty that would lead to a disproportionately risk averse response from the companies. Secondly, it fails to acknowledge that most of the major companies already do limit free expression far beyond it is limited under domestic law, and fails to propose policies to remedy this. Thirdly, it is posited as a negative obligation rather than a positive one – that is, freedom of expression is a matter for damage limitation rather than a public good to be protected and promoted.

We would like to see Government encouraging the major companies that provide our online public squares to make a commitment to develop content policies that closely reflect the boundaries set in human rights law and national law. Instead, Government is enforcing policies that would see companies exploit mass monitoring practices and limit freedom of expression far beyond the limitations in national law. As such, the White Paper's proposal for the regulator to have an "obligation to protect users' rights online" is a contradiction in terms, in the context of the harms model.

The expansive proposals aim to regulate speech across the internet

The scope of the proposals is excessively broad. The obligations would apply to any companies "that allow users to share or discover user-generated content, or interact with each other online".[63] This means, in practice, that the UK government seeks to regulate speech across most of the internet.

The Government acknowledges, though apparently without issue, that this encapsulates "a very wide range of companies of all sizes, including social media platforms, file hosting sites, public discussion forums, messaging services and search engines"[64] as well as "retailers that allow users to review products online, along with non-profit organisations, file sharing sites and cloud hosting providers."[65] This means that a duty of care would not only be imposed on everyone from Facebook, WhatsApp, Signal and Google, but also to the Mail comment section, Mumsnet, and the Boots product review

[62]Online Harms White Paper – DCMS and The Home Office, April 2019, p.56
[63] Online Harms White Paper – DCMS and The Home Office, April 2019, p.49
[64] Online Harms White Paper – DCMS and The Home Office, April 2019, para. 30, p.8
[65] Online Harms White Paper – DCMS and The Home Office, April 2019, p.49

section. In fact, if Big Brother Watch still permitted comments on our blog posts, we too would be subject to the regulation. The specific inclusion of non-profit organisations' websites and "public discussion forums" will include spaces for political and religious groups, minority groups and campaigners. This all-encompassing approach combined with the subjective notion of policing "harm" is heavy-headed, impractical and would have a chilling effect.

The proposals would further erode the right to privacy online

The breadth of the duty of care, particularly for major platforms that host millions or even billions of users, requires the companies to conduct mass monitoring. Mass monitoring and the erosion of privacy on online platforms has been the topic of major controversy in recent years, particularly because companies primarily use it for purposes associated with data profiteering. We should be very cautious of any government proposals that would, in practice, endorse such practices simply because they can serve the secondary purpose of rule enforcement. This is an unacceptable harms trade-off – and companies would be able to justify controversial, profitable data processing practices on the basis that they serve the dual function of protecting users from "harm" online.

There are several contradictory statements in the White Paper about privacy and monitoring requirements. On the one hand, it says:

> *The new regulatory framework will increase the responsibility of online services in a way that is compatible with the EU's e-Commerce Directive, which limits their liability for illegal content until they have knowledge of its existence, and have failed to remove it from their services in good time.*[66]

It also says:

> *The regulator will not compel companies to undertake general monitoring of all communications on their online services.*[67]

But on the other hand, the White Paper says:

[66] Online Harms White Paper – DCMS and The Home Office, April 2019, p.9
[67] Online Harms White Paper – DCMS and The Home Office, April 2019, p.43

> *The government believes that there is however, a strong case for mandating specific monitoring that targets where there is a threat to national security or the physical safety of children*[68]

and

> *It is therefore vital to ensure that there is the technology in place to automatically detect and remove terrorist content within an hour of upload.*[69]

It is difficult to see how these statements could be technically compatible. The White Paper does not expand on what technology should be in place and how the targeted content should be automatically detected. It would be impossible to fulfil all the duties outlined in the White Paper without conducting mass monitoring. An obligation to automatically discover potentially illegal content could constitute mass, suspicionless surveillance and also conflict with the EU e-Commerce Directive which protects companies from liability until they have knowledge of an illegal piece of content. Therefore, more clarity is required here.

Government claims that monitoring obligations will not apply to private channels,[70] but is also consulting on what constitutes a private channel and claims "users should be protected from harmful content or behaviour wherever it occurs online".[71] The problem with the consultation questions on the matter of private channels (questions 6 and 7) is that privacy has different meanings in relation to lawful content and behaviour and unlawful content/behaviour, and this White Paper wrongly tries to deal with both. This is the wrong approach.

Private communications can generally be thought of as those that are not public, and where individuals have a reasonable and legitimate expectation of privacy. However, many platforms can be used in either a public or private way. For example, some people create a Facebook profile for personal use and carefully control and limit their network and profile visibility. Accordingly, they have a reasonable expectation of privacy. Some people use closed Facebook groups to create communities, such as recovery support groups, LGBT groups, or political and religious groups where membership, visibility and participation is controlled and where users would also have a reasonable and legitimate expectation of privacy. Then again, some people use Facebook in a manner that is

[68] Online Harms White Paper – DCMS and The Home Office, April 2019, p.43
[69] Online Harms White Paper – DCMS and The Home Office, April 2019, p.13
[70] Online Harms White Paper – DCMS and The Home Office, April 2019, p.49
[71] Online Harms White Paper – DCMS and The Home Office, April 2019, p.50

completely public and have no expectation of privacy. This differentiated use is one of many reasons why generalised monitoring obligations are inappropriate and unlikely to be lawful. Generalised and indiscriminate surveillance is not lawful in relation for general crime fighting purposes (see, for example, *R (Watson) v Secretary of State for the Home Department (Case C-698/15)* – it certainly is an unacceptable method for dealing with the unbounded concept of "harm" online, whether on public or private channels.

The importance of private digital spaces

The former UN Special Rapporteur on Freedom of Expression, Frank La Rue has made clear that "throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."[72] The current UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, has expressed "the importance of privacy as a gateway to freedom of expression"[73] and noted the value of affinity-based closed groups in "protecting opinion, expanding space for vulnerable communities and allowing the testing of controversial or unpopular ideas."[74]

Many groups rely on the privacy and safety afforded by a private group in order to communicate – particularly those who experience discrimination, are vulnerable or otherwise marginalised. Many people only feel able to express themselves on the basis that their identity, what they are saying and to whom, stays within certain specific circles. This includes marginalised groups, addiction and recovery groups, sexual abuse survivor groups, and community or campaigning groups organising their work. Many of these groups operate on 'public channels' such as Facebook, but the privacy of their groups' visibility, activity and membership can be carefully managed. Imposing monitoring over such groups could have a serious chilling effect.

End-to-end encryption

In addition to the legal and rights issues, there are important technical issues to consider when imposing the "duty of care" on companies. Some companies offer structural privacy to their services – for example, the end-to-end encryption offered by instant messaging/VoIP apps WhatsApp and Signal. Interference with such companies'

[72] UN Special Rapporteur, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 16th May, A/HRC/17/27.(www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)
[73] https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf
[74] https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf

technical infrastructure is a matter of great legal and technical debate and would have a profound impact on rights. This does not mean users of such services are beyond the law – law enforcement agencies have a range of powers to seize devices, compel passwords and even covertly hack accounts and devices to circumvent end-to-end encryption.[75] End-to-end encryption does mean that the content of users' communications cannot be subjected to mass monitoring – and given the UK's commitment to upholding human rights and digital security, this is positive and should be protected.

A harm to privacy and democracy: micro-targeted advertising

The White Paper is curiously silent on one of the most significant online harms documented in recent years – micro-targeted advertising. The paper makes reference to DCMS' review of online advertising and the work of the ICO, but the omission of any proposals to deal with the issue in this framework is remarkable.

Unlike communications laws, micro-targeted advertising – particularly in the context of elections – exists in a legal and regulatory gap. Given the risk to privacy rights and democracy, this must be addressed. We concur with the ICO's call for an 'ethical pause' on the use of personal data in digital political campaigning,[76] The New Economics Foundation[77] and the Institute for Practitioners in Advertising[78] have similarly called for a moratorium on micro-targeted political advertising. Big Brother Watch believes there is a very strong argument in favour of banning micro-targeting advertising altogether.

Micro-targeted advertising online encourages data surveillance and insidious political and electoral influencing. It arguably conflicts with a number of legal and regulatory frameworks.[79] We think it has proven to be one of the greatest "online harms" in recent years as it has caused considerable anxiety about data exploitation, distrust of online spaces and even distrust of electoral outcomes, undermining democracy itself. The impact of micro-targeted advertising on democracy and social division cannot be trivialised.

---

[75] See Regulation of Investigatory Powers Act (RIPA) 2000, and Investigatory Powers Act 2016
[76] *Democracy disrupted? Personal information and political influence* – The Information Commissioner's Office, July 2018, p.45: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
[77] *Blocking the data stalkers* – M. Hall & D. McCann, New Economics Foundation, December 2018: https://neweconomics.org/uploads/files/NEF_Blocking_Data_Stalkers.pdf
[78] https://ipa.co.uk/news/ipa-to-call-for-moratorium-on-micro-targeted-political-ads-online
[79] We will make further specific submissions about this to the DCMS Committee and indeed in relation to the Online Harms White Paper if it will be considered further.

During this turbulent time in UK politics, when pivotal elections or referenda could happen at relatively short notice, we must ensure democratic processes are carefully protected – including protecting the electorate from psychographic targeting. The omission of this topic from the White Paper is very regrettable.

Digital constitutionalism: an alternative vision for a free and safe internet

Whilst we welcome the Government's attempt to rebalance power and protect citizens online, Big Brother Watch believes a root and branch rethink of this fatally flawed policy approach is required.

The proposals would erode free speech and due process norms; create an impossible two-tier system of rights online and offline that would in practice erode decades of case law and rights protections; and set a disastrous international example that would result in human rights abuses.

We would like to see Government use its power and influence to work with companies online to first adopt frameworks that reflect our constitutional and democratic values: namely, to adopt human rights and domestic law principles in their content standards, and to model enforcement on rule of law principles.

Government should encourage companies to reflect human rights principles in their approach to content regulations

Major internet intermediaries need digital constitutions that reflect the foundational values of the democracies they serve. This means content policies should reflect human rights principles and avoid limiting expression beyond the limitations of the law.

There is an evolving acknowledgement of the role businesses should play in protecting human rights. In 2008, the UN Human Rights Council in approved the "protect, respect and remedy" framework for business and human rights, resting on three core principles:

1. the state duty to protect against human rights abuses by third parties, including business;
2. the corporate responsibility to respect human rights; and
3. greater access by victims to effective remedy, judicial and non-judicial.[80]

[80] https://www.business-humanrights.org/en/un-secretary-generals-special-representative-on-business-human-rights/un-protect-respect-and-remedy-framework-and-guiding-principles

This means that whilst 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.

In 2015, the Internet Governance Forum delivered recommendations on Terms of Service and Human Rights, defining due diligence standards for platforms with regard to three components: privacy, freedom of expression and due process. When considering internet platforms and freedom of expression, those recommendations acknowledged that

> *"certain platforms should be seen more as "public spaces" to the extent that occupy an important role in the public sphere"*

and that

> *"online platforms increasingly play an essential role of speech enablers and pathfinders to information".*[81]

Clearly, major online platforms are now among the most widely used public squares. The White Paper also acknowledges, "privately-run platforms have become akin to public spaces" and have a "responsibility to be guided by norms and rules developed by democratic societies."[82] As such, Big Brother Watch believes major platforms should not censor content beyond the extent to which it would be censored under the law, which respects human rights frameworks. This position is also promoted by the Internet Governance Forum's recommendations of Terms of Service and Human Rights, which say:

> *when platforms offer services which have become essential for the enjoyment of fundamental rights in a given country, they should not restrict content beyond the limits defined by the legitimate law.*[83]

Platforms should model enforcement on rule of law principles

Platforms have to yield some power to more democratic forces, because their exercise of power requires limitation if it is to be fair. Currently, the terms of service model effectively gives most platforms absolute power and complete discretion as to their application of it. This needs to change.

---

[81] https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/830-dcpr-2015-output-document-1/file
[82] Online Harms White Paper – DCMS and The Home Office, April 2019, pp.6-7
[83] https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/830-dcpr-2015-output-document-1/file

We believe that major internet platforms should adopt rule of law principles for enforcement. Government should be promoting rule enforcement that centres transparency of rules, foreseeability of their application, fairness of processes, the right to appeal, and equal and consistent application of the rules.

Government should also work to establish processes for law enforcement to better work with companies online so that policing is not effectively privatised to unaccountable companies in Silicon Valley, but rather is a co-operative process that ultimately protects due process for citizens.

The importance of user empowerment

Unlike the physical world, users can exercise considerable control of the information and views they are exposed to online by blocking others, muting key words, controlling news feeds, and using age-appropriate controls. User control helps people to mitigate the subjective "harm" they might otherwise be exposed to. We believe companies should work to further expand and simplify user controls over the information they see, the people they are exposed to, and the recommendations they are shown. This approach protects freedom of expression in our online public squares whilst allowing people to create diverse experiences that reflect their own preferences, interests and needs.

We welcome initiatives to promote digital literacy – although we believe this is a role for our national education system rather than for tech companies. Digital literacy, combined with more effective user controls, would allow individuals to take better control of their online experiences.

Conclusion

The Government's proposals for internet regulation will set norms for new modes of social interaction; inscribe limitations on people's freedom; influence power relationships between businesses, citizens and the state; and write enduring rules into a changing world. Internet content regulations are modern speech controls that will set the parameters for the everyday interactions of billions of people. We must get it right. Unfortunately, the Online Harms White Paper is a fundamentally flawed approach – a new approach is needed.

To regulate the internet is to shape the contemporary world and the democratic rights we have within it. If this country is to demonstrate leadership, innovation and the unwavering commitment to modern democracy we expect, we must transmit the essential principles of human rights and the rule of law to the online realm. These digital constitutional values are the vital underpinnings online democratic spaces built to last.