collective wellbeing Carnegie UK

SUBMISSION TO LORDS COMMUNICATIONS AND DIGITAL COMMITTEE ENQUIRY INTO DIGITAL REGULATION

October 2021

Introduction

1. Carnegie UK was set up in 1913 by Scottish-American philanthropist Andrew Carnegie to improve the wellbeing of the people of the United Kingdom and Ireland. Our founding deed gave the Trust a mandate to reinterpret our broad mission over the passage of time, to respond accordingly to the most pressing issues of the day and we have worked on digital policy issues for a number of years.

   In early 2018, Professor Lorna Woods (Professor of Internet Law at the University of Essex) and former civil servant William Perrin started work to develop a model to reduce online harms through a statutory duty of care, enforced by a regulator. The proposals were published in a series of blogs and publications for Carnegie and developed further in evidence to Parliamentary Committees[1]. The Lords Communications Committee[2] and the Commons Science and Technology Committee[3] both endorsed the Carnegie model, as have a number of civil society organisations[4]. In April 2019, the government's Online Harms White Paper[5], produced under the then Secretary of State for Digital, Culture, Media and Sport, Jeremy Wright, proposed a statutory duty of care enforced by a regulator in a variant of the Carnegie model and this approach remains central to the Government's plans for the Online Safety Bill. France[6]. The European Commission has included a duty of care in its proposal for a Digital Services Act. We talk to frequently to our international counterparts about our work, for example in Ireland, Canada, Australia, New Zealand and the US, as well as representatives from the UN and the EU.

   In December 2019, while waiting for the Government to bring forward its own legislative plans, we published a draft bill[7] to implement a statutory duty of care regime, based upon our full policy document of the previous April[8]. We have published our initial analysis of the

1 Our work, including blogs, papers and submissions to Parliamentary Committees and consultations, can be found here: https://www.carnegieuktrust.org.uk/project/harm-reduction-in-social-media/
2 https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/29902.htm
3 https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/822/82202.htm
4 For example, NSPCC: https://www.nspcc.org.uk/globalassets/ documents/news/taming-the-wild-west-web-regulate-social-networks.pdf; Children's Commissioner: https://www.childrenscommissioner.gov.uk/2019/02/06/childrens-commissioner-publishes-astatutory-duty-of-care-for-online-service-providers/; Royal Society for Public Health: https://www.rsph.org.uk/our-work/policy/wellbeing/new-filters.html
5 https://www.gov.uk/government/consultations/online-harms-white-paper
6 French-Framework-for-Social-Media-Platforms.pdf (thecre.com)
7 https://www.carnegieuktrust.org.uk/publications/draft-online-harm-bill/
8 https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2019/04/08091652/Online-harm-reduction-a-statutory-duty-of-care-and-regulator.pdf

online Safety Bill[9] and our evidence to the Joint Committee on the Draft Online Safety Bill[10], to which William Perrin gave evidence on 23rd September 2021[11].

2. We welcome the Committee's inquiry into Digital Regulation. We set out our responses to each of the questions posed below and provide links to our work throughout, where relevant. We would be happy to speak further to the Committee members, either formally or informally, as their deliberations progress.

Question 1: how well co-ordinated is digital regulation? How effective is the Digital Regulation Co-operation Forum?

3. It is too early to judge the effectiveness of the Digital Regulation Co-operation Forum since it has only been formally in operation since April this year. And, while it brings together the main regulators responsible for many aspects of the digital world, there is little "digital-specific" regulation currently in force (with the exception of Data Protection) for it to co-operate on either.

4. How the regulatory bodies work together will in large part depend upon the personalities and incentives of their senior management - both those appointed by the Secretary of State and senior executive leaders. Government Departments making appointments should consider this in job specifications. Appointing a 'lone wolf'-type at one regulator will have a knock-on effect to the efficacy of the others and to the functioning of markets and consumer welfare. A simple change might be ensuring reciprocal duties to co-operate in digital matters as relevant legislation is amended.

5. That said, the Forum - and the Government's Plan for Digital Regulation - are a welcome first step in providing the strategic oversight and architecture required for what is a complex and fast-moving regulatory environment. The DRCF formalises a mechanism for joint working and information-sharing which was fairly well established between these three regulators (the ICO, CMA and Ofcom) in respect of "digital" issues, but which is not a totally new development; see, for example, co-operation in relation to competition (e.g. concurrency rules). We very much welcome the formal addition of the FCA from April this year. The mechanism confirms the growing priority and expanding scale of the challenge for the Government and its regulatory bodies in addressing the impact of digital technology on all our lives. The broad strategic priorities for the DRCF's first year, as set out in their 2021-22 work plan,[12] are broadly correct. The commitment to a consideration of how "planned new regimes for online regulation may interact with wider existing regulation such as financial regulation, intellectual property rights and content regulation (including advertising content regulated by the ASA)» is very welcome as is the fact that the DRCF is "considering a range of ideas about statutory support for co-operation and changes to our information-sharing arrangements".

6. However, a mechanism for joining up through a forum such as this is not – in and of itself – enough to address the harms that can emerge to users and consumers in the gaps between existing regulation nor without a mechanism to ensure that the overarching legislative and regulatory landscape, and the powers it confers on the regulatory bodies

9 https://www.carnegieuktrust.org.uk/blog-posts/the-draft-online-safety-bill-carnegie-uk-trust-initial-analysis/
10 https://d1ssu070pg2v9i.cloudfront.net/pex/pex_carnegie2021/2021/10/06120715/Evidence-Joint-Committee.pdf
11 https://committees.parliament.uk/event/5556/formal-meeting-oral-evidence-session/
12 https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122

within it, is designed to be coherent itself. We believe there is an opportunity to make this work better in relation specifically to Online Harms and would wish to see DRCF members focus urgently on this aspect so that the Government's Online Safety Bill can be as effective as possible upon introduction.

7. As per our work on regulatory interlock (see annex), we believe the draft Online Safety Bill needs to include measures which ensure the co-operation of regulators across all the harms that arise online, so that Ofcom can seek out and act on expertise and evidence of harm that sits in other regulators without becoming overburdened itself. [13]

8. A final point on the challenges for the DRCF: the Government appears to be engaged in a period of intensive strategy and policy generation across a number of digital and tech spheres. For instance, its "New Direction" proposals to reform the **Data Protection landscape** and the new **AI Strategy** have been launched since summer recess, and the AI strategy itself refers to "interconnected work of government" (p12), listing 10 examples, including: the **Plan for Growth** and recent **Innovation Strategy**; the **Integrated Review**; the **National Data Strategy**; the **Plan for Digital Regulation**; a review of the UK's **large-scale computing ecosystem**; the upcoming National Cyber Strategy; a new Digital Strategy; a new Defence AI centre; and the upcoming **National Resilience Strategy**. Add to that, the **draft Online Safety Bill**; the Home Office's imminent **Fraud Action Plan**; the long-awaited review of **Online Advertising**; BEIS's **review of competition and consumer policy**; the new **Digital Markets** regime and the **Elections Bill**, and the scale of " co-operation" required to fully cover this landscape to ensure effective "digital" regulation is apparent.

9. That said, we do not underestimate the task facing government in response to fast-paced technological changes and emerging harms associated with them; and, we commend the Government's recent "Plan for Digital Regulation" as a first step in articulating the challenge and the principles by which this will be addressed. However, we wonder whether there is enough of a strategic view, at the top of Government, as to how digital regulation should operate, what the priorities are for the UK in the next five years and the critical path to achieving it. A graphic to illustrate this (or indeed to capture all the current and planned pieces of work to understand, at a glance, the complex landscape the Government is creating) might help focus minds. Without that, the mass of strategies, policy documents and programmes of work will keep growing without the interdependencies and the impact (both on business as well as consumers) being truly assessed and evaluated, never mind the unintended consequences of reforms in one area failing to take account of existing protections in another

13 Our regulatory interlock proposal focuses on cooperation between regulators, for example where there are two regulators with different powers/duties in different fields but who need to work together to solve a problem (e.g. if FCA asked OFCOM to help on financial scams by dealing with vectors for that harm in one of OFCOM's code). Other ways of working between regulators include co-designation (mentioned briefly in the Government response to the Online Harms White Paper in Dec 2020 but not featured in the draft Bill); this is a form of delegation where OFCOM has powers/duties but asks another body to exercise them (e.g. in advertising). Another form is concurrency, where two regulators have the same responsibilities in the same field (e.g. competition in the utilities sectors).

Question 2: Do regulators have the powers and capabilities, including expertise, to keep pace with developments? What is the appropriate balance between giving regulators flexibility and providing clarity in legislation?

10. We refer the Committee to our proposal on "regulatory interlock" (see annex) which enables the growth of regulatory frameworks across a broad range of areas without overburdening one single regulator or complicating the remits of its counterparts. We are disappointed that there is no such mechanism, either for co-designation or for collaboration, within the draft Online Safety Bill, particularly given the calls for fraud, scams and the sale of unsafe or faulty products to be included in its scope and the clear case made by the FCA, City of London Police and other financial sector bodies for action in these areas. The Government is right not to want a "Christmas Tree Bill" nor to sink Ofcom with a remit that is too broad too soon; our proposal would however enable the wider regulatory system in the UK to work together to address the real and present harms that occur to online users (and, applied more broadly, to all customers and citizens whose lives are impacted in any way by digital technologies) and to build in the future-proofing and flexibility required to keep pace with developments.

11. However, we would flag to the Committee that the Government's intentions, as set out in its recent "Plan for Regulation" may not be entirely congruent with the Committee's concern about regulators keeping pace with developments. Under one of the Plan's three main principles - to "actively promote innovation" - it notes that "we will seek to remove unnecessary regulations and burdens where possible". While we are not advocates of unnecessary regulation by any means, we do ask whether the government feels that there is already enough *necessary* regulation in a sector where issues relating to data privacy and data protection, surveillance, algorithmic bias, unfair competition and a lack of consumer protection all need to be better addressed. There is also the risk introducing gaps or contradictions if regulations are removed too quickly or without taking account of the wider strategic purpose. Regulation can provide a secure space for innovators to work and allow more risky innovation than would be publicly acceptable in controversial areas, while taking account of the fact that people are rightly concerned about data protection and safety of children and young people.

12. There are two stand out examples of this in the UK flowing from regulation of human fertilisation and embryology. The early 1980s Warnock framework that limited experimentation on human embryos allowed that experimentation to proceed without public backlash. Then, 15 years, later the team at Roslyn was able to clone a mammalian embryo with little public disquiet working in an ethical regulatory framework that drew on the 1980s breakthrough. By contrast, Dolly the sheep was greeted with some horror in the USA, with President Clinton questioning whether we should 'play god'. The UK science establishment learned a great deal from scientific innovation failures in the 1990s, in particular GM foods where public confidence was lost due to the perceived lack of a regulatory framework. This led to a tight, innovation-minded adaptation of the precautionary principle to inform regulators by a UK cross-government committee which we commend to the Government[14]

14 See ILGRA paper here; https://webarchive.nationalarchives.gov.uk/ukgwa/20190701152341/ https://www.hse.gov.uk/aboutus/meetings/committees/ilgra/pppa.htm The application of the precautionary principle to decisions on regulation of emerging technology is also discussed in our full reference paper (2019): https://www.carnegieuktrust.org.uk/publications/online-harm-reduction-a-statutory-duty-of-care-and-regulator/

Applying the precautionary principle in relation to the regulation of novel technologies is advisable: it is perfectly possible to regulate to protect against harm to consumers while encouraging innovation.

13. The UK has also seen some tragedies in experimental facilities where controls may have been lax - the 2007 foot and mouth disease outbreak from Pirbright Laboratories, the 1977 Dounreay sodium explosion scattering radioactive material around the local area (still causing problems decades later) and - admittedly a special case – the Windscale Fire. Without rigorous safety standards modern versions of such events could occur, in particular as software is increasingly embedded in physical devices - cars, drones, weapons etc.

14. The UK is well-placed to learn from regulatory successes enabling innovation and innovation that went too far leading to a public backlash - regulation should always consider how to help innovators not lose public confidence. And, regulation for innovation should not undermine the physical safety of workplaces and the duty to others affected by the workplace set out in the statutory duty of care in the Health and Safety at Work Act 1974.

15. Clarity in detailed legislation is particularly illusory in fast moving fields such as digital. Parliament can't make specific laws fast enough to keep up. This is why Carnegie advocates for a statutory duty of care which provides an overarching framework within which innovators can take decisions to innovate while not harming the public.

Question 3: How effective is digital regulators' horizon scanning? How could this be improved?

17. The DRCF plan of work identifies a number of live and emerging issues, and the CMA is an exemplar in identifying sources of consumer harm, compiling evidence and pushing the Government to respond.

18. However, horizon-scanning is not the necessarily the pressing issue here. As set out above, the proliferation of proposals, consultations, strategies and reviews has not been matched by any real progress in developing or implementing any actual regulation. The Online Safety Bill has been four years in development (since proposals were first mooted in the Internet Safety Strategy in 2017) and we are still a number of years away from the regime being operational. There is still a tendency within Government - much encouraged by the social media companies, as well as start-ups and tech industry trade bodies - to deem that regulating technology is "too difficult" (our work has consistently argued that it isn't). We do not argue that it is easy, but we wonder if the proliferation of "activity" across all the products Government is publishing is at best making the conceptualisation and design of effective regulation harder, and at worst, creating a diversion that suits the tech sector but fails consumers and users of digital services. There is also an inherent tension at the heart of DCMS between its dual objectives to support the growth of the UK tech sector and to protect consumers, whether across cyber security, data protection, digital markets or online harms. The Department is uniquely susceptible to sustained lobbying on the latter during its regular engagements with tech companies and trade bodies on the former - a lobbying that is opaque and unseen by the civil society and other representatives who wish to see greater

regulatory progress on the latter objectives. We have no doubt that DCMS civil servants wish to make equal progress on both Departmental aims but the playing field on which they are offering Ministerial advice is far from level.

Question 4: How effective is parliamentary oversight of digital regulation?

19. Carnegie UK submits to many digital-related inquiries by Parliamentary committees. We judge from that perspective that greater focus and the pulling together of work might help Parliament's oversight. There is much merit in Lord Gilbert's suggestion at a recent Joint Committee hearing[15] that a standing Committee in Parliament should be established to monitor the implementation of the Online Safety Bill. Indeed perhaps this could go further and shadow the DRCF. We would also draw the Committee's attention to the risks where Parliamentary oversight is reduced in favour of increasing powers taken by the executive, as is the case in relation to the powers granted to the Secretary of State in the Online Safety Bill. We attach in the annex our blog[16] on this subject and will be providing amendments to the Bill shortly to address this.

Question 5: What is your view of the Committee's proposal in Regulating in a digital world for a "Digital Authority" overseen by a joint committee of Parliament

20. We are strongly against the establishment of any new bodies to take forward regulation.[17] The government's focus has to be on getting on with regulation itself, not the distraction and costs of establishing new organisations and the significant disruption and impact on productivity in the existing regulators as they move into new working practices. in this regard, the DRCF is a sensible step - allowing existing, highly experienced regulators, competent within their own jurisdictions, to cooperate and identify shared priorities on an equal footing without undertaking a disruptive and prolonged reorganisation of roles, responsibilities and staff. A further consideration is the fact that - given "digital" now spans all sectors and all industries, with barely an individual in the country who is not in some way affected by how it is regulated - bringing "digital" together in one place would potentially mean splitting up other policy areas (such as competition, data protection and consumer protection) which span both "digital" and "non-digital" spheres.

Question 6: How effectively do UK regulators co-operate with international partners? How could such co-operation be improved?

21. With respect to the international dimension (again specifically focused on Online Harms), we would draw your attention to the relevant section from our submission to the joint Committee on the Online Safety Bill[182] and recommend the fuller arguments set out in our evidence to the Tech and Foreign Policy inquiry[19]. In post-Brexit Britain, we are yet to find out whether we shall be a rule-setter or a rule-taker (as Singapore styled

15 https://committees.parliament.uk/event/5556/formal-meeting-oral-evidence-session/
16 https://www.carnegieuktrust.org.uk/blog-posts/secretary-of-states-powers-and-the-draft-online-safety-bill/
17 See our full reference paper "Online harm reduction: a statutory duty of care and a regulator" (2019); p56 Available here: https://d1ssu070pg2v9i.cloudfront.net/pex/pex_carnegie2021/2019/04/06084627/Online-harm-reduction-a-statutory-duty-of-care-and-regulator.pdf
18 https://committees.parliament.uk/writtenevidence/39242/html/
19 https://committees.parliament.uk/writtenevidence/35708/html/

itself decades ago). If we have aspirations to be a rule-setter, this will require assiduous work by regulators in international forums working closely with FCO to ensure they have correct Diplomatic support from posts and missions (as our evidence to the FCO committee inquiry points out the UK is lacking in diplomatic representation for digital.

Carnegie UK, October 2021
Contact: maeve.walsh@carnegieuk.org

Annex A

Online Harms - Interlocking Regulation (blog published 10 September 2020; https://www.carnegieuktrust.org.uk/blog-posts/online-harms-interlocking-regulation/)

The statutory duty of care approach to online harms gives regulators a new route to protect the vulnerable and make markets work better where social media might have caused harm. The statutory duty approach focuses on systemic issues with social media services rather than individual complaints or breaches. Many regulators encounter the use of social media to breach rules they administer and these could also constitute breaches of the statutory duty of care at a systemic level. The Online Harms White Paper uses the example of social media to sell knives or other age-restricted goods to minors – and the problems might be more effectively dealt with through that route. While action on individual user complaints remains with these regulators, enforcement of the statutory duty of care lies with OFCOM, the government's likely online harm regulator. To avoid overburdening OFCOM, provide a simple path for the other regulators and certainty for companies and victims, some sort of process is needed to manage the interlocking of regulatory regimes.

This blog post proposes a system of regulatory interlock based on existing principles of regulatory co-operation, which is light touch and maintains focus on systemic issues not individual cases. Over the operational lifetime of Online Harms legislation there will be pressure to add (and possibly remove) issues to the scope of regulation – describing a system at the outset provides for orderly growth or shrinkage. We also suggest issues that require further thought which we will deal with in subsequent posts.

Online Harms Regime

We refer in this document to the regime we set out with Carnegie UK Trust in a draft Bill in late 2019 which proposed amendments to the Communications Act 2003. The Carnegie model is of online platform services subject to a statutory duty of care to prevent reasonably foreseeable harms arising to people as a result of the operation of those services. OFCOM is the regulator we proposed to enforce this systemic regime. A systemic regime does not generally deal with individual cases but looks at service design and business operation. The government's Online Harms White Paper sets out a similar regime.

Context

All of life (if not everyone in the world) is on the Internet, and even more specifically on social media platforms. "In real life" Parliament has created many specialist regulatory systems to prevent harm to people and make markets work better in many sectors – for example, food, trading standards, financial services, or elections. These specialist regimes complement and sometimes engage both the criminal and civil law. The way social media have been designed or are operated sometimes make it hard for these regulatory regimes to protect people and allow markets to function. Regulators complain that they do not have a route to influence social media platforms in relation to the operation of their regimes[1] even when harm appears to be being caused by the operation of social media services. The e-commerce directive (which the UK appears likely to retain after Brexit) specifically allows duties of care to be imposed upon service providers.

How does a general online harm regulator like Ofcom and the companies subject to the duty, address harms evidenced or foreseen in other specialist regulatory regimes? We know from Ofcom research[2] that the top four online harms experienced by adults (spam, fraud/scams, hacking/security, data/privacy) all are addressed in part by other regimes (criminal, regulatory and civil). This data suggests that those regimes are not working well.

Conversely, how can OFCOM, the general online harm regulator tap into the expertise of specialist regulators? How do the specialist regulators identifying online harms tap into the statutory duty of care? There are of course precedents from other areas of regulation for systems of nominating lead regulators and regulators working together[3] and OFCOM already works with many other regulators in many different ways from full concurrency to simple co-ordination. From these examples, we have developed a model for interlocking regulation.

Interlocking regulation

We propose a mechanism that allows or requires regulators to work together on issues that fall within a specialist regime but also constitute or contribute to harm within the online harms regime. Allowing formal 'interlocking regulation' would help both victims and social media companies have more certainty about how regimes work than an ad hoc approach. In such a system, OFCOM should only be considering evidence of systemic harms presented by another regulator, not adjudicating an individual fraud, scam or other case, which remains the responsibility of a specialist regulator.

As part of the online harms, legislation Ofcom would be obliged to consider complaints about systemic issues from regulators designated in legislation.

National regulators such as the Financial Conduct Authority or the Food Standards Agency would likely be on the list which could be added to from time to time by statutory instrument. Where many regulators operate in parallel at a local level, such as Trading Standards Services (TSS) then OFCOM could follow a process analogous to the Regulatory Enforcement and Sanctions Act (RESA) and ask Trading Standards services to nominate a body to raise systemic issues on behalf of all TSSs. Some regulators do have the competence to act systemically on social media services – notably the ICO and CMA. These regulators would not need to use this mechanism because of this competence; the existing mechanisms for cooperation/ concurrence will continue unaffected.

Ofcom would be empowered to determine the details of the process, including format of a complaint process, supporting evidence etc. The essential elements of any such process would indicate the nature of the problem, together with evidence of level of incidence and how it arises. It may be that the specialist regulator could suggest which elements of the regulated service are contributing to the problem, but that determination lies in OFCOM's remit. The specialist regulator should demonstrate evidence of dialogue with the regulated service, even if that is one-sided, and set out an assertion of the systemic issue enabling the harm to happen.
The process could work like this: a local TSS identifies cases of a type of scam perpetrated repeatedly using a social media platform that has led to complaints through their regulatory regime and harm to customers. The TSS has raised this with the online harms regulated platform but the scam continues; insofar as the platform has made any attempt to deal with the issue it has been unsuccessful. The TSS suspects that there is a systemic failure to prevent

harm, perhaps with weak KYC allowing repeat offences from scammers (as they republish on the platform under another name after being shut down) or a perpetrator is using the system as intended and causing harm (e.g. targeting ads to vulnerable groups), but the platform operator had not thought this through at the design stage. The TSS presents this in a dossier to OFCOM through the nominated route to begin a dialogue with OFCOM about the alleged systemic problems leading to harm. OFCOM's role is to examine this systemic issue only. OFCOM does not adjudicate individual cases/instances of harm. The burden is on the specialist regulator to present the case clearly enough with sufficient evidence that OFCOM can assess the strength of the case and have enough information to understand the nature of the problem.

An effective interlocking regulatory approach reduces the load on OFCOM – and they would not have to maintain a standing force of experts in areas covered by other regulatory regimes as they might under concurrency of powers. It provides a manageable route for OFCOM to work with other regulators building on its track record of regulatory co-operation. Current OFCOM enforcement guidelines allow it to launch investigations on receipt of information from other regulators and even to consider whether other regulators should do an investigation instead.[4] OFCOM also has concurrent Competition Act powers over postal and communications markets and experience liaising with the CMA. The new Digital Regulation Cooperation Forum arising from the CMA report into digital advertising markets, heralds a new, substantial area of regulatory co-operation. The regulatory interlock process could feed into the new Forum or vice versa.

This regulatory interlock approach would fit into the Carnegie draft Bill. The draft Bill does not limit the scope of harms. To allow for regulatory interlock on systemic issues as above requires a clause that requires OFCOM to define after consultation a process to receive and assess evidence from regulators established in law of systemic harms arising from the operation of regulated services. This could be similar to draft clause 8 where a 'super complaint' process is described. While the super complaint mechanism is different from regulatory interlock, it does provide a point where recognised civil society actors can formally interact with the regulatory system. In this, there are similarities between the mechanisms.

The government suggests in the White Paper and the interim response that 'consumer' harms would be excluded. It has been explained to us that this is due to perceived complexity of OFCOM's task. We suggest that the model above removes concerns about complexity and would fit well with the government's commitment to a systemic approach which we understand might not define harms on the face of the Bill. If there is no limitation on scope of harms, then a clause as described above could enable interlock in a manageable way.

Annex B

Secretary of State's powers and the draft online safety Bill (blog published: 14th September 2021; https://www.carnegieuktrust.org.uk/blog-posts/secretary-of-states-powers-and-the-draft-online-safety-bill/)

The draft Online Safety Bill gives too many powers to the Secretary of State over too many things.[1] This is a rare point of unity between safety campaigners, who want tough legislation to address hate crime, mis/dis-information and online abuse[2] and radical free speech campaigners who oppose much of the Bill.

To meet the UK's international commitments on free speech in media regulation, the independence of the regulator from Government is fundamental. This boundary between the respective roles of the Government and the regulator in most Western democracies is well-established. The United Kingdom is party to a Council of Europe declaration that states that national rules for a broadcasting regulator should:

> "*Avoid that regulatory authorities are under the influence of political power.*"

The United Kingdom was also party to a 2013 joint statement on freedom of expression between the Organisation for Security and Co-operation in Europe (OSCE) (of which the UK is a participant), the Office of the United Nations High Commissioner on Human Rights, the Organisation of American States and the African Commission on Human and Peoples' Rights. In that statement, made at a time of great international regulatory change due to the move to digital transmission, the United Kingdom also agreed that:

> *"While key policy decisions regarding the digital terrestrial transition need to be taken by Government, implementation of those decisions is legitimate only if it is undertaken by a body which is protected against political, commercial and other forms of unwarranted interference, in accordance with international human rights standards (i.e. an independent regulator)."*

The United Kingdom has been a leading exemplar of the independent regulator approach. In the Communications Act 2003, Parliament set OFCOM a list of objectives for setting its standards codes, then leaves OFCOM to set the codes without further interference or even having to report back to Parliament. This is a good demonstration of the balance referred to in the OSCE statement. Parliament and government set high-level objectives in legislation then do not interfere in how the regulator does its day-to-day business.

With the Digital Economy Act 2017, Parliament agreed that Government could direct OFCOM, but that power was limited to exclude OFCOM's content rules. The Wireless Telegraphy Act 2006 powers of direction also do not touch content.

Unfortunately the draft Online Safety Bill deviates from these sound principles and allows the Secretary of State to interfere with OFCOM's independence on content matters in four principal areas. The draft Bill gives the Secretary of State relatively unconstrained powers to:

- set strategic priorities which OFCOM must take into account (cl 109 and cl 57)

- set priority content in relation to each of the safety duties (cl 41 and 47)
- direct OFCOM to make amendments to their codes to reflect Government policy (cl 33)
- give guidance to OFCOM on the exercise of their functions and powers (cl 113).

The UK Government has not explained why the Secretary of State needs these powers. We propose that the draft Online Safety Bill provisions relating to these powers should be amended to create a more conventional balance between democratic oversight and regulatory independence to underpin freedom of expression.

Parliament and Government set OFCOM's initial priorities

Parliament and Government, working with the traditional checks and balances, should be able to set broad priorities for OFCOM's work on preventing harm. We understand that OFCOM would also welcome initial prioritisation, as would regulated companies. Victims' groups also want reassurance the harms that oppress them will be covered by the legislation. Parliament will want to be confident in what OFCOM will do with the powers being delegated to it.

However, the Secretary of State's powers should not cross the line in the Digital Economy Act and permit the Government to direct OFCOM on content matters through Statutory Instruments (SIs). Clauses 109 and 57 do so on strategy (albeit with some Parliamentary oversight in cl 110) and cl 41 and cl 47 on Priority Content. These extensive powers enable detailed government influence on the implementation of policy, potentially influencing decisions that impact content, and undermine OFCOM's independence.

A better balance can be struck between Parliament and the executive in setting priorities that maintain OFCOM's independence. We suggest examining the issue in two parts: regime start up; and response to issues during operation. The draft Bill should be amended so that:

- the Secretary of State specifies (with supporting research) the initial outcomes they seek to address and 'priority content' on the face of the Bill, which Parliament can hold to account. This sets priorities during the regime start-up phase.

- during regime operation, changes to priority content should originate from OFCOM's research, not from the Secretary of State, and be rigorously evidence-based. OFCOM should form the need for new priority content from its research, then consult Parliament, the Secretary of State and others. OFCOM should have regard to the consultation and present a report to the Secretary of State from which they should make a Statutory Instrument (by the positive procedure) to put the new priority content into effect.

The Secretary of State should periodically (every three years) be able to give OFCOM an indication of their strategic priorities for Internet Safety, but this should not cut across into content, nor into OFCOM's day-to-day administration.

Parliament and government then respect OFCOM's independence

The draft Online Safety Bill envisages a continuing control in the hands of the Executive beyond high level strategic direction. Clauses 33 and 113 affect OFCOM's role to implement policy; the OSCE statement is particularly clear that this should be an area in which there is no Government interference. Yet both clauses cross the boundary emphatically. Moreover, there is no attempt to provide for scrutiny or control of these powers by Parliament. The Secretary of State's power to direct OFCOM to make amendments to the code to reflect Government policy (cl 33) and to give guidance as to the exercise of functions and powers are simply egregious and should be deleted.

i For example, see evidence given to the Home Affairs Select Committee on 3 June 2020 by the City of London Police and the National Economic Crime Centre https://www.parliamentlive.tv/Event/Index/6f8da59b-0daf-473d-90f7-4dde9509dfc7

ii See page 45 of chart pack https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-of-harm-online

iii See for instance http://www.legislation.gov.uk/ukpga/2008/13/contents

iv OFCOM 'Enforcement Guidelines for Regulatory Investigation' includes references to other regulators as being alternative routes of action and sources of information that might trigger an investigation 'whether there are other alternative proceedings that are likely to achieve the same ends, or deal with the same issues, as the potential investigation. This could include, for example, whether other agencies may be better placed to investigate the complaint or whether planned market reviews may address the potential harm;' …
'and in response to information provided to us by other bodies (for example, where other regulatory bodies, MPs, consumer organisations or the press draw our attention to complaints they have received about a particular issue).
https://www.ofcom.org.uk/__data/assets/pdf_file/0015/102516/Enforcement-guidelines-for-regulatory-investigations.pdf Recently the ICO, CMA and Ofcom have announced a Digital Regulation Co-operation Forum (https://www.gov.uk/government/publications/digital-regulation-cooperation-forum)