CarnegieUK TRUST

CHANGING MINDS • CHANGING LIVES

Submission to Joint Human Rights Committee Inquiry

January 2019

1. This submission to the Joint Human Rights Committee Inquiry does not focus specifically on issues relating to data use, data privacy and the implications for human rights. The implications of the digital revolution on Article 8 are not limited to data privacy. Article 8 is a very broad right. The European Court of Human Rights described it as covering:

> *"an individual's physical and social identity, including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world".*[1]

The rights so protected are not just negative rights, protecting the individual from state intrusion, but can constitute positive obligations on the state. In addition to regulating for data protection and informational privacy, States are also under an obligation to ensure respect for individuals' psychological integrity[2] – which could include taking action against a range of harms (e.g. cyber-bullying, addiction). Consequently we put forward a regulatory approach which is relevant to the third question in the Terms of Reference on regulation of technology, whether the focus of the regulation is on data use or data privacy (as per the remit of this inquiry) or other online harms caused, for example by interactions on social media or other platforms:

> *"What regulation is necessary and proportionate to protect individual rights without interfering unduly with freedom to use and develop new technology".*

Background

2. Lorna Woods (Professor of Internet Law, Essex University) and William Perrin (Trustee of Carnegie UK Trust) have been working with Carnegie UK Trust (CUKT) to design a regulatory system to reduce harm on social media. The proposals have been published via a series of blog posts [3] and in detailed evidence submitted to the ongoing Lords Communications Committee Inquiry ("The Internet: to regulate or not to regulate?")[4]. A new paper has recently been published which updates our thinking in the light of feedback and discussions with diverse stakeholders.[5]

1 Tysiqc v Poland App no 5410/03 ECHR 2007-I; Botta v Italy App no 21439/93 ECHR 1998-I.

2 Glass v United Kingdom App no 61827/00 ECHR 2004-II [74]–[83].

3 https://www.carnegieuktrust.org.uk/project/harm-reduction-in-social-media/

4 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/the-internet-to-regulate-or-not-to-regulate/written/82684.html

5 https://www.carnegieuktrust.org.uk/publications/internet-harm-reduction/

3. We have vast experience in regulation privacy and free speech issues. William has worked on technology policy since the 1990s, was a driving force behind the creation of OFCOM and worked on regulatory regimes in many economic and social sectors while working in the UK government's Cabinet Office. He ran a tech start up and is now a trustee of several charities. Lorna is Professor of Internet Law at University of Essex, an EU national expert on regulation in the TMT sector, and was a solicitor in private practice specialising in telecoms, media and technology law.

4. Our Carnegie work was catalysed by the harms set out in the government's Green Paper[6] and much reporting of harms by interest groups. We published our work just before the government's May 2018 announcement that they would bring forward a White Paper (now expected this spring) that will:

> *'set out plans for upcoming legislation that will cover the full range of online harms, including both harmful and illegal content. Potential areas where the Government will legislate include the social media code of practice, transparency reporting and online advertising.'*[7]

5. Our work feeds into the policy debate that has ensued. Indeed, the case for regulation got stronger during 2018. We believe the challenges facing policymakers and legislators around how to rebalance data use and data privacy in favour of individuals' right to privacy have a parallel in the challenges of addressing the proliferation of online harms – all falling with the scope of Article 8. The traditional approach of not regulating innovative technologies needs to be balanced with acting where there is good evidence of harm but there has not been enough time to establish indisputable evidence of the existence of harm and its causation. We see this as a core challenge for establishing and operating a new regulatory regime.

6. A well-established approach to assessing the desirability of regulation in the face of a plausible but still uncertain risk of harm is the precautionary principle. In the UK, after the many public health and science controversies of the 1990s, the government's Interdepartmental Liaison Group on Risk Assessment (ILGRA) published its version of the precautionary principle aimed at decision makers:

> *'The precautionary principle should be applied when, on the basis of the best scientific advice available in the time-frame for decision-making: there is good reason to believe that harmful effects may occur to human, animal or plant health, or to the environment; and the level of scientific uncertainty about the consequences or likelihoods is such that risk cannot be assessed with sufficient confidence to inform decision-making.'* [8]

7. The ILGRA document advises regulators on how to act when early evidence of harm to the public is apparent, but before unequivocal scientific advice has had time to emerge, with a particular focus on novel harms. The ILGRA's work is still current and hosted by the Health and Safety Executive (HSE), underpinning risk-based regulation of the sort we propose.

6 https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper

7 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf

8 http://www.hse.gov.uk/aboutus/meetings/committees/ilgra/pppa.htm

8. Another consideration in any discussion of technology regulation is where the accountability lies for the emergence of the particular harms, or the consequences to individuals of using a particular service. We have revisited Lawrence Lessig's work from 1999[9]. Lessig observed that computer code sets the conditions on which the internet (and all computers) is used. While there are other constraints on behaviour (law, market, social norms), code is the architecture of cyberspace and affects what people do online: code permits, facilitates and sometimes prohibits. It is becoming increasingly apparent that it also nudges us towards certain behaviour. While Lessig's work was oriented along a different line, it reminds us that the environment within which harm occurs is defined by code that the service providers have actively chosen to deploy, their terms of service or contract with the user and the resources they deploy to enforce that. Service providers could choose not to deploy risky services without safeguards[10] or they could develop effective tools to influence risk of harm if they choose to deploy them. This "by design" approach is already enshrined in data protection, where GDPR requires organisations essentially to " 'bake in' data protection into processing activities and business practices, from the design stage right through the lifecycle."[11]

9. In sum, online environments reflect choices made by the people who create and manage them; those who make choices should be responsible for the reasonable foreseeable risks or consequences of those choices – whether it's psychological harm to vulnerable individuals caused by interactions on social media, or unacceptable breaches of privacy as a result of companies' collection and use of data.

A duty of care

10. The high-level details below set out in broad terms how the duty of care would apply to harm reduction on social media – our primary focus in our work for Carnegie – but we believe its application can be much broader, covering the impact of other emerging and innovative technologies and their use. Crucially, we also set out below how the duty of care can protect individuals without interfering unduly with freedom to use and develop new technology. Further detail is set out at the references above and we would be delighted to provide further information to the Committee, either in writing or as oral evidence.

11. Social media platforms are forms of public spaces. People go to such platforms for all sorts of activities and, while using them, should be protected from reasonably foreseeable harm as they would expect in any public place, such as an office, bar or theme park. While some places are subject to specific regimes (e.g. pubs), other rules apply more generally, for example the Occupiers Liability Act and the Health and Safety at Work Act 1974 each of which impose a statutory duty of care. This concept is straightforward in principle and well-established. A person (including companies) under a duty of care must take care in relation to a particular activity as it affects particular people or things. If that person does not take care, and someone comes to a harm identified in the relevant regime as a result, there are legal consequences, primarily through a regulatory scheme but also with the option of personal legal redress.

9 See Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach", (1999), 113 Harv. L. Rev. 501; also "Code and Other Laws of Cyberspace" (1999) and "Code: version 2.0" (2006)

10 'God only knows what it's doing to our children's brains. The thought process that went into building these applications, Facebook being the first of them, … was all about: How do we consume as much of your time and conscious attention as possible?' (Sean Parker, a Facebook Founder, 2007) https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html

11 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

12. Applying the "duty of care" approach to the social media sphere has a number of significant benefits:

- It is simple, broadly-based and largely future-proof – expressed in terms of outcome (the prevention of harm) not specifics of process.[12]
- The regulatory approach is essentially preventative, reducing adverse impact on users before it happens, rather than a system aimed at compensation/redress.
- The categories of harm can be specified at a high level, by Parliament, in statute.[13]
- It would apply to all social media service providers accessible in the UK regardless of size, with the regulator taking a proportionate approach according to the severity of harm and the size of risk, as well as the size of service operator. Online services from traditional media companies would be out of scope.
- A risk-based regulatory approach provides for safe system design (including operational and business choices). (For example, the GDPR emphasis on privacy by design sets basic design conditions for all services, regardless of size and the ICO's Age Appropriate Design Code is an example of developing good practice in this regard.)
- It is compatible with EU law including the eCommerce Directive and minimises collateral damage to freedom of speech.
- In micro economic terms returns external costs to the production decision and is efficient if applied in a manner proportionate to risk of harm.

How would it work?

13. New legislation would set out the duty of care and identify the key harms Parliament wants the regulator to focus on. We suggest that those harms would be: the 'stirring up of hatred offences', national security, harms to children, emotional harm, harms to the judicial and electoral processes, economic harms. While these categories would be established in statute, work would need to be done on the scope of each of the harm. It could be that this work would be delegated by the act to an independent regulator which would operate in a transparent and evidence-based manner.

14. We envisage the tasks of such a regulator to be:

- provide guidance on the meaning of harms;
- support best practice (including by recognising good practice in industry codes);
- gather evidence;

12 The government recently confirmed that the 1974 duty of care in the Health and Safety at Work Act applies to artificial intelligence software employed in the workplace. https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2018-05-23/HL8200/

13 See Health and Safety at Work Act 1974 S2: http://www.legislation.gov.uk/ukpga/1974/37/section/2

- encourage media literacy;
- monitor compliance; and
- take enforcement action where necessary.

15. We suggest that the regulator runs a harm reduction cycle[14], involving civil society as well as companies at each consultative step. The regulator would begin by requiring companies to measure and survey harm, produce plans to address these harms for public consultation and agreement with the regulator then the companies implement the plans. If the cycle does not reduce harms or the companies do not co-operate then sanctions could be deployed.

Balancing regulation with innovation

16. We note that the Committee specifically frames its question on regulation in relation to developing and using new technology. Some commentators have suggested that applying a duty of care to all providers might discourage innovation and reinforce the dominance of existing market players. We do not think that the application of the duty of care would give rise to a significant risk in this regard, for the following reasons.

17. Good regulators do take account of company size and regulation is applied proportionate to business size or capability[15]. We would expect this to be a factor in determining what measures a company could reasonably have been expected to have taken in mitigating a harm. Clearly, what is reasonable for a large established company would be different for an SME. The 2014 statutory 'Regulators Code[16]' even requires some regulators to take a proportionate, risk managed approach to their work, the code says that:

> *'Regulators should choose proportionate approaches to those they regulate, based on relevant factors including, for example, business size and capacity.'*

18. The proportionality assessment proposed does not just take into account size, but also the nature and severity of the harm, as well as the likelihood of it arising. For small start-ups, it would be reasonable for them to focus on obvious high risks, whereas more established companies with greater resources might be expected not only to do more in relation to those risks but to tackle a greater range of harms.

19. The regulator should determine, with industry and civil society, what is a reasonable way for an SME service provider to manage risk. Their deliberations might include the balance between managing foreseeable risk and fostering innovation (where we believe the former need not stymie the latter) and ensuring that new trends are taken account of by other companies in a timely fashion.

20. We note that, in other sectors, regulators give guidance on what is required by the regulatory regime and ways to achieve that standard. The ICO has done just that in relation to the implementation

14 Detailed blog post on harm reduction cycle: https://www.carnegieuktrust.org.uk/blog/social-media-harm-regulator-work/

15 HSE - 'For many businesses, all that's required is a basic series of practical tasks that protect people from harm and at the same time protect the future success and growth of your business.' http://www.hse.gov.uk/simple-health-safety/

16 The Code does not apply to OFCOM but sets out Government views on good regulation - https://www.gov.uk/government/publications/regulators-code

of GDPR. This saves businesses the cost of working out how to comply. In addition to guidance as to what risks are likely and immediate steps to mitigate those risks (provided in easier to understand language, perhaps even decision trees), another way to support companies would be the development of libraries of 'good code' that provide appropriate solutions to some of the most common problems.

21. Furthermore, regulators would not be likely to apply severe sanctions in the case of a start-up, at least initially. A small company that refused to engage with the regulatory process would presumably become subject to more severe sanctions.

Who should regulate?

22. The government, OFCOM, the ICO and countless lobby groups have described serious harms occurring now apparently at a population scale. Data collection and use has also become a high-profile, politicised issue as a result of the Facebook/Cambridge Analytica scandal and subsequent examples of misuse of personal data. In considering structural regulatory options, weight should be giving to doing things quickly.

23. The duty of care proposal is based on a well-understood regulatory approach that could be legislated and deployed quickly. Our proposals revolve around risk management. The regulator would need to prioritise its work based on risk management. In setting priorities, the regulator would consult civil society, industry the public and parliament, much as existing regulators do. The regulator would not be able, nor would it wish to implement the entire regime from day one but would require a judicious phasing based on risk. The regulator would be dealing with far fewer companies than the ICO or the HSE.

24. We have argued that the role implementing the statutory duty of care for social media should be given to OFCOM; should a duty of care be applied to elements of data protection, use and data privacy, then consideration would need to be given to the role of the ICO and the intersection of the duty of care regulation with the Data Protection Act. If the regulator has new responsibilities it will require more resources. Resources to support regulation should still be provided on a "polluter pays" basis – either from the proposed internet services tax or from a new industry levy.

25. In either scenario, whether regulating social media harms or those arising from data privacy breaches, we see no need for a new regulator to implement a statutory duty of care. A new super regulator will be complex to legislate and deploy;[17] and, in a turbulent climate, where Parliamentary time is focused on Brexit and political distractions are rife, it is likely impossible to achieve in anything less than five years.

William Perrin

Lorna Woods

17 William Perrin (as a DTI civil servant in 2001) devised the paving Bill approach that created OFCOM: OFCOM was proposed in the Communications White Paper in December 2000, created in a paving act in 2002 but did not vest and become operational until December 29 2003 at a cost of £120m (2018 prices).