Written evidence from CARNEGIE UK TRUST SUBMISSION (TFP0014)

1. We welcome the Committee's inquiry and the opportunity to submit evidence. Carnegie UK Trust has played a major role in developing UK policy on internet safety regulation and helped organise an international Pathfinder Group of NGOs on Internet Safety for Technology Ministers meeting under the UK Presidency of the G7.

Tech and Foreign Policy: priorities for the UK

2. We believe the priorities for the UK (including the FCDO) should be:

- Demonstrating that democracies have a strong role in governing the internet instead of leaving it to global companies and unelected technologists. HMG should export the UK Online Safety approach, including the statutory duty of care, developed by Carnegie UK Trust, and now found elsewhere, notably the EU.

- New, strong multilateral processes for competent democratic governments to work together on technology governance embedding human rights principles, securing democratic debate and correcting market failures. The first step was the G7 tech ministers' declaration secured by Oliver Dowden[1]. This might require a new treaty.

- Deploy democratic technology governance as a bulwark against autocratic technology governance– such as the China's World Internet Conference - and defending democracy itself from strategic online disinformation campaigns by hostile state actors, their proxies and fellow travellers that threaten national security.

- Embracing governments that do not have the technical capacity to make their own rules in multilateral processes- similar to observer status at Basel and through systems like a reinforced Commonwealth Cyber Declaration and Rule of Law programmes.

- Improving the byzantine, even chaotic UN process (WSIS etc) by external leadership demonstrating how to do it better.

For the FCDO this means:

- identifying a structure to help DCMS manage a sustained drive of technology diplomacy over the next five years.

- Identifying who at Ambassadorial (SMS4 level or equivalent) is responsible for the landscape of tech regulation and what resources do they command.

[1] https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration

- Developing a system for assessments of disinformation campaigns by foreign actors that threaten national security to be shared for action between the intelligence services, companies regulated under the Online Safety regime and the regulator.

In summary:

3. The history of international internet technology governance is based on a 1990s era presumption that this was best left to companies and technologists. Governments had little role and were regarded by many as harmful. This led to a baroque set of structures for internet governance and standards-setting based on contracts between companies rather than treaties between governments. While the multistakeholder model can be seen as a solution, as currently established, is problematic. "Legitimacy can be weak, costs of participation are high, developed countries and industry tend to dominate, processes are slow and rambling, and overall participation is low."[2] A contract-based model gave rise to issues about enforcement, especially cross border and with asymmetries of bargaining power. The public interest is not easily brought into focus in such a model. The weakness of the current UN approach has led to a multitude of different initiatives, with different emphasises.[3] The absence of governments in this space led to a strategic move by China to set up its own technology standards and governance groups that reflect Chinese values – notably omitting human rights.

4. Rules from the 1990s in the USA and in the EU limited the liability of online platforms for the things that people did with them. Traditional law enforcement agencies around the world found it hard to enforce the law online. Some of this may have been due to resourcing of law enforcement, to the difficulties of cross-border enforcement but some of it may have been down to the fact that online platforms (and other intermediaries) had little incentive to cooperate.

5. In the last five years democratic governments have begun to appreciate the extent of harms that arise to citizens and businesses from an only loosely ungoverned internet. The UK is a leader, forming a matrix of regulators between the Competition and Markets Authority, the Information Commissioner's Office, the Financial Conduct Authority and OFCOM[4] and bringing forward Online Safety Legislation. The UK's approach to Online Safety is based upon work done by Carnegie UK Trust in 2018 – the so-called Woods-Perrin model[5]. The EU parallels much of the UK work in the Digital Services Act[6]. Australia and Canada are also about to regulate. The UK has gone from a perhaps exposed position of proposing a modern regulatory regime to being the leader of a pack of nations all determined to regulate.

---

[2] E. Taylor, ICANN: Bridging the Trust Gap (Global Commission on Internet Governance Paper No 9), March 2015, available: https://www.academia.edu/35815665/ICANN_Bridging_the_Trust_Gap, p. 4.
[3] The post 'Internet Governance Outlook 2021: Digital Cacaphony in a Splintering Cyberspace' By Wolfgang Kleinwächter Professor Emeritus at the University of Aarhus is a strong overview of the state of play. https://www.circleid.com/posts/20210108-internet-governance-outlook-2021-digital-cacaphony/
[4] https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum
[5] https://www.carnegieuktrust.org.uk/project/harm-reduction-in-social-media/
[6] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

6. The issues are pan-national – at present the business activities of several Chinese and USA companies cause negative externalities in a wide range of other countries. In the future, which nation's technology companies cause problems in which other countries may change. In microeconomic terms this has similarities to cross border factory pollution issues addressed by a range of treaties in the 1970s and early 1980s despite the prevailing cold war.

7. The Joint Ministerial Declaration of G7 Technology Ministers was a notable victory for the UK Chair Oliver Dowden and his Sherpa team. For the first time, the G7 governments acknowledged jointly that online safety was an issue. It was particularly significant that the Biden administration was able to sign up to this – Biden has committed elsewhere has committed to a taskforce to investigate online violence against women and girls[7].

8. Carnegie UK Trust, Reset.Tech, Institute for Strategic Dialogue and The German Marshall Fund of the USA worked together to support G7 Deliberations convening an internet safety pathfinder group of NGOs for the UK Chair.

9. The G7 process reminds us that there is nowhere for democracies to discuss how they regulate technologies in the (democratically determined) public interest and in international human rights norms. This isn't something that the OECD supports and regulation goes well beyond the G7 and the EU states (Von Der Leyen has made several entreaties to the USA for bilateral USA/EU talks on the 'tech rule book' that have so far not been acknowledged).

10. The G7 Technology Ministers' statement stops short of proposing a new mechanism for international discussion of technology regulation. Former US diplomat Anja Manuel proposed a T-10 group of democracies[8] with a focus on technology standards to counterbalance China's standards work. Google employee and former State Department diplomat Jared Cohen proposes[9] a medium-sized grouping of democracies to discuss technology issues that he styles T-12. However, he is vague about what it should do; a Googler is quite unlikely to recommend co-ordinated multi-national regulation. Steve Feldstein of Carnegie Endowment for International Peace points out that a technology grouping without a clear agenda and that leaves out say Africa and most of Asia would not be very effective[10].

11. Manuel, Cohen and Feldstein were writing before the April 2021 G7 technology Ministers' declaration which now opens the door for a multilateral focus on technology regulation.

12. The Online Safety Bill in the UK and the DSA process in the EU will demonstrate the huge issues that arise from regulation. As over 90% of the countries/blocs regulating are dealing with externalities caused by foreign companies' international co-ordination is vital. This will require a robust, well-staffed international mechanism rather than a series

[7] https://joebiden.com/vawa/
[8] https://www.ft.com/content/bc7abf86-f13e-4025-a120-004361aef21a
[9] https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies
[10] https://www.cfr.org/blog/how-should-democracies-confront-chinas-digital-rise-weighing-merits-t-10-alliance

of ad-hoc meetings around the G7. It is possible that the Cohen T-12 could form the core of such a body but with the explicit agenda of discussing regulation of online safety. Other issues could be added on later.

13. The group could operate on a core and observer status (addressing Feldstein's criticism). Democracies with technical capability should set the pace but other nations and bodies should routinely be allowed to participate as Observers who may also contribute – similar to how we understand the Basel financial regulation structures operate[11]. The FCDO could use the Commonwealth Cyber Declaration[12] as a vector for engagement or the Commonwealth Good Laws Project which shares model legislation across the Commonwealth.

14. The United Nations has sought to restart its work on internet governance via the Internet Governance Forum[13] but it has made no meaningful reforms to the IGF which was itself a legacy of a company-led governance process.

15. It is presumably part of the point of the Committee's inquiry to establish from where in the FCDO activity such as this is led. In a modern, networked Whitehall DDCMS should play an important role. But ensuring that the FCDO has someone at a senior Ambassadorial role with a staff to support and drive the diplomacy as part of the Department's overall mission is vital.

16. FCDO should also play a leading role in developing a system to handle assessments that a strategic disinformation campaign is underway that could be a significant threat to national security. In the Government's Final Response to the consultation on the Online Harms White Paper the government said:

> *'Where disinformation and misinformation presents a significant threat to public safety, public health or national security, the regulator will have the power to act.'*

17. The assessment of such a threat from a foreign country, to – say - a UK election (as the USA intelligence authorities assessed[14] to the 2020 USA election), would involve the FCDO and its intelligence agencies. However, evidence of the significant threat to national security arising from disinformation could come from one of the companies regulated under the Online Safety regime or a specialist NGO, who informs the regulator OFCOM or another of the digital regulators. At present, information transmission is through informal, opaque channels: this creates two problems, both the impacts on rights and democratic legitimacy and the lack of clarity as to whether the system is effective. In a formal regulatory regime, where there are commercial consequences for regulated companies, a formal more transparent process will be required for sharing and action upon threat information. The UK government has not set out how they intend

---

[11] See http://www.basel.int/TheConvention/OpenendedWorkingGroup(OEWG)/Meetings/OEWG11/AdmissionofObservers/tabid/7507/Default.aspx

[12] https://thecommonwealth.org/commonwealth-cyber-declaration

[13] https://www.intgovforum.org/multilingual/

[14] https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public

such a system to work in the new Online Safety regime. The FCDO should play an important role in resolving this problem.

About our work

18. The Carnegie UK Trust 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.

19. 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[15]. The Lords Communications Committee[16] and the Commons Science and Technology Committee[17] both endorsed the Carnegie model, as have a number of civil society organisations[18]. In April 2019, the government's Online Harms White Paper[19], 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[20]. 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 Canada, Australia, New Zealand and the US, as well as representatives from the UN and the EU.

20. In December 2019, while waiting for the Government to bring forward its own legislative plans, we published a draft bill[21] to implement a statutory duty of care regime, based upon our full policy document of the previous April[22]. We now await the Government's draft Online Safety Bill and will continue our policy development and advocacy work in response.

Carnegie UK Trust

May 2021

---

[15] 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/
[16] https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/29902.htm
[17] https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/822/82202.htm
[18] 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
[19] https://www.gov.uk/government/consultations/online-harms-white-paper
[20] French-Framework-for-Social-Media-Platforms.pdf (thecre.com)
[21] https://www.carnegieuktrust.org.uk/publications/draft-online-harm-bill/
[22] https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2019/04/08091652/Online-harm-reduction-a-statutory-duty-of-care-and-regulator.pdf