Submission to the Consultation on the Online Harms White Paper

1. Introduction

The Global Network Initiative (GNI) welcomes the opportunity to engage in the government of the United Kingdom's consultation on its Online Harms White Paper. Over the last two years, GNI has held several meetings with representatives of the Foreign & Commonwealth Office, the Home Office, and the Department of Digital, Media, Culture & Sport to discuss the government's concerns about online harms.[1]

GNI shares the government's concerns about the need to preserve and improve the safety of Internet users, especially children. We also appreciate the government's stated commitment to a free, open, and secure Internet, as well as its intention to continue to protect freedom of expression online.

GNI is the world's preeminent multistakeholder collaboration in support of freedom of expression and privacy in the information and communication technology (ICT) sector. GNI's members include leading academics, civil society organizations, ICT companies, and investors from across the world. All GNI members subscribe to and support the GNI Principles on Freedom of Expression and Privacy ("the Principles"), which are drawn from widely adopted international human rights instruments. The Principles, together with our corresponding Implementation Guidelines, create a set of expectations and recommendations for how companies should respond to government requests that could affect the freedom of expression and privacy rights of their users. The efforts of our member companies to implement these standards are assessed by our multistakeholder board.

The approach outlined in the White Paper represents a significant change to the existing domestic regulatory context that could have profound impacts on the international landscape as well. We urge the government to more carefully consider the potential impacts this change could have on existing voluntary efforts, such as the Global Network Initiative, as well as broader international dynamics. As set out in more detail below, we are also concerned that the approach outlined in the White Paper is both too broad and unnecessarily vague. We ask the government to take the time necessary to narrow and flesh-out its approach in more detail, in broad consultation with all stakeholders, before moving forward with legislation in order to protect freedom of expression online, promote innovation and competition, and provide the coherence and certainty that the government seeks to deliver.

[1] In addition to private meetings with these agencies, GNI organized two invitation-only roundtables in London on content regulation with UK and Europe-based stakeholders on October 6, 2017 and March 28, 2019.

2. International context: The need for practical, proactive, and proportionate leadership

As the White Paper acknowledges, a number of other governments have recently enacted or are seriously considering regulations to address various types and forms of online content. GNI and its members are tracking and engaging with these initiatives in dozens of countries around the world and have a keen sense of how these disparate efforts risk creating overlapping and conflicting laws, leaving companies to arbitrate between competing legal frameworks.

In particular, the combination of the European Union's decision to reopen the e-Commerce Directive and the UK's pending exit from the EU creates the potential for parallel reforms to existing intermediary liability regimes within Europe. In order to ensure coordination and clarity, we encourage the government to explain how it will engage on these matters in Brussels and elsewhere going forward.

GNI supports the government's desire to "lead towards new, global approaches for online safety that support [the UK's] democratic values, and promote a free, open and secure internet." In order for this vision to be realized, and to ensure that the government's efforts are not cynically used by others to silence critical voices, we believe it must be firmly grounded in the globally recognized laws and principles set out in the international human rights framework.

Those laws and principles require government actions that restrict freedom of expression to meet the following conditions: legality (they must be established through democratic processes and be sufficiently clear as to provide notice and be predictable); legitimate purpose (they can only be enacted for certain, specific purposes set out in relevant international human rights treaties); and necessity (they must constitute the least restrictive means for achieving the aforementioned legitimate purpose, and be proportionate to the interest being protected).

3. Recommendations to ensure an appropriate regulatory approach

It is important that, post-consultation, the broad approach outlined in the White Paper is refined into more specific and concrete requirements. As the government moves forward in its consultations on and consideration of the approach set out in the

White Paper, we recommend that the above-mentioned principles and the following key concepts inform those efforts:

- Users' rights – for the government to demonstrate values-based leadership on this issue, a human rights framework must be embedded into government decision-making and design of policy that results from this consultation. The government must put users' human rights at the forefront of its efforts and ensure that any restrictions on the freedom of expression and privacy of Internet users are clearly and precisely defined in any ensuing legislation, strictly necessary, carefully considered, narrowly tailored, and fit for purpose. They must also be accompanied by effective grievance and remedial mechanisms.
- Inclusiveness – we welcome the governments' focus on the needs of specific, vulnerable groups, including children. However, we urge the government to carefully consider the rights of all Internet users, including those who may not be represented by vocal advocacy groups, so as to fully explore and mitigate any potential, unintended consequences of measures proposed to protect such groups.
- Transparency – we welcome the government's efforts to facilitate greater transparency among Internet companies, as well as its own commitment to publishing its first transparency report. We urge the government to ensure that these efforts are carefully coordinated to help users understand the information being reported, to avoid a proliferation of distinct, national reporting criteria and/or formats, and to mitigate unnecessary costs and confusion.
- Accountability – the proposed regulatory framework would grant a significant amount of authority and discretion to a regulator, without setting out in sufficient detail how that regulator will be kept accountable. We are particularly concerned about the ability of the regulator to prohibit categories of content that are not clearly defined to be illegal by law, to develop burdensome and potentially contradictory guidance across this wide range of "harms", and to levy significant penalties, which could create incentives for companies to overly censor content and thereby limit freedom of expression. It is therefore vital that the powers of this authority be carefully considered, narrowly defined, and competently overseen.
- Innovation and competition – we encourage the government to continue to carefully consider and mitigate the impacts that regulation may have on innovation and competition. Particular attention should be paid to the cumulative effect of such a sudden move to complex statutory regulation and

other digital policies on the diversity of the digital ecosystem in the UK and future investment. The government must give further consideration to the potential adverse impacts that its proposed approach may have on start-ups and smaller companies.[2] While we appreciate the commitment to enshrining "the principle of proportionality" in law and understanding what may be "reasonably practicable" for particular companies based on their size and resources, we are nevertheless concerned that the broad range of content and significant penalties contemplated could prove detrimental to newer and smaller companies' ability to attract investment and take innovative risks.

- Redress – the White Paper's focus on "user redress" is laudable. However, the focus appears to be primarily, if not exclusively, on ensuring that companies provide appropriate mechanisms for users to "raise complaints and concerns about harmful online activity" and "to alert the regulator to an alleged breach of a company's duty of care." Implementing legislation and regulatory clarification must also pay due regard to users whose rights to freedom of expression and privacy may be adversely impacted by the regulatory approach.

4. Areas of particular concern

a. Scope of application

i. Companies in scope of the regulatory framework

The White Paper proposes to take an ambitious approach to implementing an admittedly new and untested approach to content regulation. We fear this approach is unnecessarily broad, and that it is likely to undercut the governments' laudable focus on protecting freedom of expression, while making the regulator's duty to pay due regard to innovation difficult, if not impossible.

The scope of application, applying to any "hosting, sharing and discovery of user generated content" *and* any "facilitation of public and private online interaction" that "provide services to UK users," sweeps an incredibly wide range of services and platforms into the remit of regulation. Yet the examples of harms cited in the White

[2] The White Paper refers to "companies in scope of the regulatory framework" without defining what is understood by "companies". We assume that the conscious use of this term indicates a desire to exclude non-profit platforms and service providers, including academic institutions, virtual libraries/repositories, and efforts to document human rights violations.

Paper appear to focus on a relatively small set of social media services. The broader and deeper this new regulatory approach applies, the greater the potential for, and possible implications of, any unintended consequences that may emerge. The government's assertion that "[h]armful content and behaviour … cannot readily be categorised by reference to a single business model or sector," is unsupported by evidence and the broad approach envisioned is inconsistent with those being discussed and implemented in other jurisdictions.

We encourage the government to start with a narrower focus. Evidence demonstrating that a clearly defined, substantial risk, impact, and/or harm exists on a particular service or type of service should be a prerequisite for regulatory coverage. Indeed, the risk-based approach to regulatory action set out in Section 5 of the White Paper provides a possible framework for defining the scope of regulation (as opposed to prioritization of enforcement) around specific services and platforms which are having the greatest impacts and present the greatest risk of harm.

This more focused approach will be more efficient for the regulator to enforce and minimize the potential chilling effects that regulation could otherwise have on freedom of expression, privacy, innovation, and investment. If, after some experience policing these narrow categories, a clear and compelling case emerges for an expanded approach, the government will then have the evidence needed to justify and tailor additional regulations to further areas of concern.

Finally, we strongly support the government's attention to the importance of privacy, as well as its commitment that "any requirements to scan or monitor content for … illegal content will not apply to private channels." However, it remains unclear what would be expected of companies that provide private messaging services, and how any such obligations could be implemented without risk of violating user privacy and/or data protection regulations.

ii. Harms in scope

The White Paper identifies as in scope any "…online content or activity that harms individual users, particularly children, or threatens our way of life in the UK…" The list of "harms with a clear definition" is composed mostly of familiar, albeit disparate categories of illegal content. Even here, where definitions and factors relevant to determinations of illegality often exist in law and related jurisprudence, many questions remain as to how a regulator will interpret what constitutes "reasonably practical" efforts for the broad range of Internet services covered. The government's approach also

requires private companies to make determinations as to the legality of particular online content, outsourcing a role that has and should be reserved, as a matter of principle, to accountable, public authorities.

The separate category of "harms with a less clear definition" also raises serious concerns. The challenge of objectively defining what constitutes "coercive behaviour," "intimidation," or "disinformation" in a way that provides clarity and predictability to both companies and users will be significant, if not impossible. Even where the regulator is able to establish clear, tight definitions and guidance for these categories (notwithstanding the exhortation in the White Paper for *less* "specific and stringent requirements … for those harms which may be legal but harmful"), significant risk will remain that content falling within those parameters may nevertheless constitute speech which is legal and/or protected by the right to freedom of expression.

If faced with ambiguity and uncertainty, as well as significant penalties, companies – especially those that are under-resourced – are likely to default toward content restriction so as to minimize their risk of liability, thereby threatening freedom of expression. That tendency is likely to be exacerbated if companies face dozens of different codes for different types of content, each with their own distinct and potentially conflicting guidance and/or requirements. It remains unclear how this can be reconciled with the regulator's obligation to protect users' rights online, including by ensuring "that the new regulatory requirements do not lead to a disproportionately risk-averse response from companies that unduly limits freedom of expression."

We are concerned that regulator will not only be charged with developing and enforcing codes for the 23 categories of "online harms" identified in the White Paper, but also with enforcing the "duty of care" "even where a specific code does not exist," and unilaterally identifying and defining new categories of harm beyond this "initial list." The degree of discretion and lack of unpredictability such a system would create is highly concerning. Going forward, we urge the government to focus initially on those harms that are already established by statute as illegal and have clear definitions. To the extent other harms are seen as sufficiently serious as to require regulation, they should be deliberated upon openly and defined through legislation. Furthermore, given the substantial authority of this new regulator, the government should create robust oversight and accountability mechanisms to ensure that it is acting pursuant to the public interest and consistent with its obligations.

b. Duty of care

The framework set out in the White Paper is centred around a "duty of care" on relevant companies "to take reasonable steps to keep their users safe and tackle illegal and harmful activity on their services." This legal concept is borrowed from other areas of law, which differ in significant ways from the online environment. Most scenarios in which a duty of care has been established statutorily or under common law do not create a responsibility for one party to police the behaviour of a second party vis-à-vis a third, much less to prevent harm to collective concepts such as "national security" or "shared rights".

As the White Paper explains, "[t]his statutory duty of care will require companies to take reasonable steps to keep users safe, and prevent other persons coming to harm *as a direct consequence of activity on their services*" (emphasis added). As proposed, and in particular as applied to non-illegal content, this "duty of care" concept risks creating a false trade off and encouraging (indeed, perhaps requiring) companies to prioritize the "safety" of some users over the freedom of opinion and expression (including the right to receive information) of others.

In sum, rather than making the Internet in the UK safe, the awkward application of a "duty of care" to the regulation of user-generated content online, combined with the unnecessarily broad range of companies and harms in scope, the relatively-unfettered power and discretion of a still-unknown regulator, and the looming threat of draconian sanctions for non-compliance, risks making the Internet in the UK significantly more sterile, cautious, and silent.

5. Conclusion

We remain committed and look forward to continuing to engage with the government on its efforts to address online harms. We do not deny the significance of the harms under consideration, or the urgency with which the government encourages companies to act to address them. However, we fear that the proposed regulatory framework risks creating significant new costs (to the digital economy in the UK, to freedom of expression and privacy, and to the UK's potential to demonstrate global leadership) without necessarily effectively tackling the harms it sets out to address.

The approach outlined in the White Paper would establish a new, formidable regulatory function, without establishing any clear checks and balances on its authority. This authority would be allowed to oversee an incredibly diverse range of Internet services, from video game platforms, to web hosts, to search engines. The regulator

would be empowered not only to define "codes of conduct" for the broad set of very different categories of "harms" set out in the White Paper, but also to unilaterally (or, in some instances, in collaboration with law enforcement, but in all cases potentially independent of Parliament) establish new categories, without any discernible criteria as to what evidence-base, consultation process, and/or cost-benefit analysis is required. The regulator would also be given almost complete discretion to enforce these "codes" with some of the most significant regulatory tools in the government's toolkit, such as service disruption and/or blocking, as well as criminal liability.

These unprecedented powers are likely to create significant threats to freedom of expression by incentivizing companies to censor otherwise protected speech. The government should take steps to narrow and more clearly define its regulatory approach, before the ideas set out in the White Paper are emulated by others who do not share its laudable vision.