GNI Statement to the House of Lords on Freedom of Expression and Privacy Issues in the Draft Online Safety Bill

As a contribution to ongoing deliberations of the House of Lords on the UK Online Safety Bill (the Bill), the Global Network Initiative (GNI) writes to share key considerations and concerns. As this legislation moves toward finalization, GNI encourages the Lords to prioritize amendments which ensure an appropriate and proportionate scope of substantive obligations, oversight and enforcement authorities, penalties for noncompliance, and privacy safeguards, including vis-a-vis end-to-end encryption.

GNI is a multistakeholder initiative that brings together 90 leading information and communication technology (ICT) companies, civil society organizations, academics, and investors, collaborating around a shared framework for the protection of freedom of expression and privacy in the ICT sector. GNI has been engaged throughout the Bill's evolution, first providing input on the consultation on the White Paper in July 2019. Following the government's response to this consultation, GNI held a multistakeholder roundtable in September 2020 with key actors in the UK. GNI has continued to maintain dialogue with UK policymakers on the bill, including through evidence presented to the Foreign Affairs Committee of the House of Commons in November 2021.

As we emphasized in our initial submission, GNI shares and appreciates the UK Government's commitment to the safety of individuals online, especially children, and we acknowledge the limited references to freedom of expression and privacy in various provisions in the Bill. However, notwithstanding the narrowing of the scope of companies and content covered by the bill over time, significant digital rights risks remain. As drafted, the Bill is likely to place undue pressures on ICT companies to restrict the rights to freedom of expression and privacy in the UK and undermine existing commitments to responsible company decision making.

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org

The recommendations and analysis below is informed by GNI's global experiences advocating for rights-respecting content regulation policies and convening regular multistakeholder consultations in support of the framework detailed in GNI's Content Regulation and Human Rights Policy Brief. We detail several areas for improvement: ongoing concern with the duty of care model: the broad scope of duties for illegal and harmful content fail to provide sufficient guidance for companies tasked with enforcement and individuals using products and services;

- Risk of disproportionate enforcement: resulting from pairing the duties with overly burdensome penalties, including potential criminal liability for company personnel, and providing. insufficient oversight of and transparency from the regulator;
- Privacy risks: in particular the obligations that may undermine the use of end-to-end encryption;
- Freedom of expression risks: throughout the bill, additional safeguards are needed to ensure companies, the government, and Ofcom prioritize freedom of expression protections.

As detailed below, GNI acknowledges several proposed amendments from the House of Lords addressing some of these concerns. We stand ready to engage with the Lords throughout the Committee stage deliberations in support of such amendments and we welcome opportunities to share GNI's multistakeholder perspective in support of rights-respecting content regulations.

I) Ongoing Concerns with the Duties of Care

In GNI's initial submission to the White Paper, we shared concerns about the duty of care model and the scope of harms and companies covered. Although the Bill has since changed significantly, its obligations still risk pushing a broad range of companies toward more restrictive approaches to speech and conduct than is otherwise allowed in the analog space, as well as excessive monitoring of users' communications. We appreciate that the bill references "proportionate measures" for implementing safety obligations, and establishes duties covering freedom of expression and privacy, transparency measures, and appeals and reporting

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org

mechanisms, among others. However, many of these duties — in particular the duties regarding freedom of expression and privacy rights — do not carry the same weight as the companies' other responsibilities under the bill. This is further imbalanced by the Bill's stringent enforcement provisions for overbroad duties relating to addressing illegal and harmful content online. We encourage the Lords to support the many amendments that strengthen safeguards for individuals' and children's rights.

Safety Duties — Illegal Content

The safety duties for addressing illegal content feature both proactive duties for preventing or limiting access to priority illegal content and reactive duties for removing broader illegal content, which apply to both "user-to-user" and search services. The proactive duties introduce the risk of proactive monitoring by companies of users' communication, while requiring companies to remove certain categories of speech likely fails to meet the standards of legality and legitimate purpose that should underpin any restrictions on expression. Priority illegal content in the bill includes terrorism, child sexual exploitation material, and the offences detailed in Schedule 7, some of which are nebulous and difficult to address through a proactive approach or strictly through take-down or leave-up decisions, further incentivizing over-removal. This includes the offence (including conspiracy, aiding, and abetting) of "assisting illegal immigration."

In addition, the current threshold for companies to infer illegality, i.e., "reasonable grounds to infer, on the basis of all information reasonably available to it, that the content is illegal" (Clause 170, in the Bill as brought from the House of Commons[1]), is overly broad. Companies have obligations to remove or limit the risk of encountering such content upon becoming aware of it, as well as to respond to user reports of alleged illegal content (e.g., Clauses 9, 16, and 23). We call on the Lords to further clarify this threshold for identifying illegal content, acknowledging

[1] Clauses referenced in this analysis are taken from the HL Bill 87-EN as brought from the House of Commons

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org

proposed amendments to better align with thresholds for commission of offences under criminal law. We also encourage the Lords to reject broadening the scope of priority illegal content, noting particular concerns about applying this scope for the proposed "false communications offence."

Safety duties — Harmful Content

The updated "triple shield" approach, which moves away from legal but harmful content duties for adults, still places companies' implementation of their terms and conditions under the purview of the regulator. These terms are often global in nature and can be more restrictive than local laws on certain content issues, which creates a general risk of overbroad and/or extraterritorial enforcement. To help mitigate some of these enforcement risks, we appreciate the proposed amendment to ensure these systems and policies are not enforceable by statute in the UK, and encourage a focus on transparency of companies policies, systems, and enforcement instead. Beyond illegal content duties and compelled implementation of company terms of service, a broad range of companies must also implement mitigation measures for risks of harm to individuals (broadly defined) that they identify as part of risk assessment, or which Ofcom otherwise identifies in codes of practice or other guidance (e.g., Clauses 8, 9, 22, 23, 36, and 89). In addition to the tiered obligations and some of the exemptions for services detailed in Schedule 1, we encourage the Lords to further narrow and tailor the obligations to appropriate services, paying particular attention to the implications for public interest platforms, smaller/micro businesses, community-led moderation approaches, and internet infrastructure providers.

Services 'likely to be accessed by children,' must also undertake extensive child safety risk assessment and safety duties, including mitigating the risks of harm to children and preventing children from encountering any content which may be harmful to them, using measures such as age assurance (Clauses 10,11, 24, and 25). Assessing and addressing potential safety risks on

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org

platforms and services are critical aims that GNI supports, but the current model fails to provide sufficient guidance for users to understand the bounds of acceptable speech on platforms and legal clarity for platforms tasked with enforcing those boundaries.

Furthermore, the implementation of these duties rests on platforms knowing the age of their users, requiring potentially invasive collection of personal data — such as ID or facial scans — even for simply accessing information online. We welcome the amendments that would ensure that the Bill does not mandate platforms to use age verification technologies or otherwise require that their use is accompanied by rigorous safeguards and clear guidance from Ofcom. We also encourage the Lords to ensure that the bill does not require platforms to remove speech that would otherwise be legal in order to comply with child safety duties on harmful content.

Freedom of Expression and Privacy

GNI recognizes and appreciates the call for companies to have particular regard to protecting users' right to freedom of expression when putting in place safety measures and policies (Clauses 18 and 28). However, when contrasted with the more robust safety duties established in the Bill (and the heavy sanctions regime enforcing its compliance), this wording is not sufficiently strong to ensure freedom of expression and privacy rights are given due consideration. We encourage the Lords to strengthen these principles amid the significant countervailing duties that will be placed upon companies.

We appreciate the call for Category One services to measure and assess potential freedom of expression and privacy risks related to the safety measures they examine and adopt, and even to publish these assessments, where appropriate, (Clause 18). The GNI Framework, and the broader, complementary UN Guiding Principles on Business and Human Rights (UNGPs), include robust guidance for how companies can undertake such assessments. Where such assessments

might surface actual or potential human rights impacts, the GNI framework helps companies identify steps they can take to prevent, mitigate, and remedy adverse impacts. We are encouraged by further amendments that set out matching duties for Ofcom to hold special regard to freedom of expression and privacy in assessing the guidance they provide to platforms.

2) Oversight and Enforcement

As indicated above, the duties for safety measures regarding illegal content, mitigating risks of harms (broadly defined), and protecting children's safety, are in and of themselves arduous, but they are made more concerning due to the overly broad enforcement powers and excessive penalties Ofcom can administer under the Bill. Given these penalties and Ofcom's dual hats in both providing additional guidance and serving as the primary body tasked with enforcement, the Lords should provide additional criteria for penalties under the Bill, as well as further transparency obligations for Ofcom.

Overly Burdensome Penalties

The Bill allows Ofcom to assess fines of up to 10 percent of global revenue on covered entities, as well as to obtain court orders against third parties to deny noncompliant entities business facilities, including on an interim basis, or, as a last resort, to block them within the UK. While these maximum penalties will of course not be applicable in every case, the threat of such a significant "stick" is likely to lead to over-enforcement by companies. As detailed in Clause 119, the range of "enforceable requirements" are applicable for nearly the full range of duties in the Bill, subject to limited exceptions detailed in Schedule 13, and Ofcom appears to have broad leeway in identifying the penalties they deem appropriate for particular violations (e.g. Clause 127(5)).

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org

Ofcom also has substantial data collection authority via information notices they can administer to companies in assessing companies' implementation of the duties in the Bill (e.g. Clauses 92–97). Given these substantial investigative powers, the Lords should strive for amendments that require Ofcom to engage with the public and civil society to design and communicate clear expectations in any guidance it develops, and to issue proportionate penalties for companies in scope in line with these expectations. As a start, this might include building upon existing requirements in the Bill for Ofcom to issue annual reports (Clause 116) and publish enforcement measures (Clause 136). GNI emphasizes transparency and ongoing multistakeholder engagement as effective components of rights-respecting content regulation, and we encourage Ofcom to model these practices should the Bill move ahead.

Personnel Liability

In the current draft, these significant penalties are paired with potential liability for company personnel for non-compliance with information notices, both within and outside of the UK. The draft Bill details obligations for a senior manager legally responsible for compliance with the notices, (e.g., Clause 94, Clauses 98-102, and Schedule 12). (Notable is Clause 98(4), which could penalize an officer for failing to provide communications in an unencrypted format in response to a notice). GNI has responded to the growing trend of potential liability for company personnel under content regulation in various jurisdictions, noting that without sufficient safeguards and protections, such requirements make it less likely that companies will push back on overbroad government approaches.

We are also concerned about the potential impacts of proposed amendments which would broaden the scope of individual criminal liability for senior managers for non-compliance with a range of duties under the bill, including Clause 11 on child safety duties. As colleagues at GPD have illuminated, the broad nature of the duties described in Clause 11 would provide insufficient guidance for personnel facing criminal liability, likely failing to uphold the principle

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org

of legality that should underpin any restrictions on the right to freedom of expression. This could contribute to disproportionate impacts, whether through significantly limiting children's access to services (and thereby infringing upon childrens' rights), overuse of content filtering tools for otherwise legal content, or even companies leaving the UK market. The Lords should carefully consider whether criminal liability in this context is necessary and proportionate, given the variety of tools that the UK government has at its disposal to compel compliance. If criminal liability is imposed, the Bill should be amended to ensure that this only happens in limited circumstances following significant breaches of the law, following an escalation process that ensures sufficient notice and opportunities to comply.

Secretary of State's Authority

Under the bill, the Secretary of State has significant enforcement authority as well as the ability to set out additional guidance and expectations for online Speech. Of particular concern is the Secretary of State's ability to designate primary priority content that is harmful to children (content which companies must prevent access to or minimize the risks of children encountering under the safety duties in Clause 11 and 25), the ability for the Secretary of the State to give orders to Ofcom under "special circumstances" akin to emergency scenarios (Clause 156), and the ability for the Secretary of the State to cite "public policy reasons" as a basis for recommending modifications to codes of practice from Ofcom (Clause 39), among other authorities.

In regulating matters of online speech, it is important to create a certain level of independence between officials, regulatory bodies, and the public, given the risks of stifling political criticism and debate where governments shape such requirements. Category One providers must implement specific protections for content in the public interest and journalistic content (Clauses 13–15), and it's important that government officials are not able to shape or influence definitions or decisions on this type of content to protect freedom of expression rights in digital

communications. GNI appreciates and encourages consideration of the amendments that have been proposed to narrow these powers.

3) **Privacy Risks**

As we have noted throughout this submission, the duties encouraging platforms to proactively address "priority illegal" and "primary priority content harmful to children," paired with the potential for significant penalties for non-compliance, raise real concerns for the disproportionate monitoring of users. Digital rights experts have expressed concern about information collection that may be required to implement requirements even under the new "triple shield" model in the bill, including "age-gating" and identity verification. We encourage amendments from the Lords that articulate ways to address risks and potential harms without requiring the use of tools for monitoring communications or proactive detection and removal of broad swathes of user content at risk of legal penalties for noncompliance. The information notices and potential for extensive access to company data by Ofcom, as described above, also raise data protection and transparency considerations.

Ultimately, the privacy risk of most concern is the potential for Ofcom to issue notices under Clause 110(2) that will require companies to use accredited technologies to identify Child Sexual Abuse (CSEA) material, not only on public communications, but on private (and potentially encrypted) channels as well. As a general matter, GNI is concerned about the necessity and utility of such an approach, as well as the precedent it would set by empowering a regulator to require the use of specific technologies and/or direct research and development spending of private companies.

GNI has long expressed the critical importance of encryption and anonymity in enabling freedom of expression. Digital rights experts have expressed concern about companies' ability to comply with this requirement without undermining critical privacy protections on encrypted communications services. At a time where encryption is under threat in various global

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org

regulatory contexts, it is imperative that the UK finds ways of addressing legitimate content-related concerns without undermining the security and privacy of individuals' communications.

Conclusion

The House of Lords has a responsibility to help ensure that the Online Safety Bill protects freedom of expression and privacy. While we appreciate the government's intention to ensure safety online, as drafted, the broad reach of providers' duties, paired with insufficient guidance and overly stringent penalties for noncompliance, place undue pressure on companies to restrict access to content and services and monitor user activity. The House of Lords has an important opportunity to strengthen critical safeguards for freedom of expression and privacy in the Bill (including commitments to preserving encryption), to require additional transparency and multistakeholder engagement from Ofcom, and to push for more flexible, proportionate, and iterative approaches to enforcement. Amendments along those lines will also help ensure consistency with the UK's broader foreign policy leadership as a global champion of human rights, a member of the Freedom Online Coalition, and a signatory of the Declaration on the Future of the Internet, and we stand ready to engage with UK policymakers in support of these aims.

1325 G St. NW, Suite 500, Washington, DC 20005 • GlobalNetworkInitiative.org • info@GlobalNetworkInitiative.org