Online Harms White Paper: Open Consultation Submission

Brad Hanlon, Lindsay Gorman, Bret Schafer
The Alliance for Securing Democracy

SUMMARY

Since almost its inception, the online information commons has been under attack from an array of actors, foreign and domestic. As malign actors erode truthful and civil discourse online, key foundations of liberal democracies are at stake. Certainly, internet companies share a portion of the responsibility for this state of affairs. But regulating overzealously risks undermining the principle of free expression that democratic societies champion. In order to increase the effectiveness of the Online Harms White Paper's response to these far-reaching challenges and protect our values worldwide, future legislation should:

1) Reassess the risks of adopting such a wide scope for regulation based on ill-defined "harms," and address the need for solutions that are both tailored to the individual threats themselves and that take into consideration the nature and capabilities of different online platforms.

2) Reassess the efficacy of empowering a government regulator to oversee action against such a wide range of challenges and ensure that any such regulator maintains a clear and proportionate enforcement structure, as well as credible independence from the government.

3) Define "private communications" or "private channels" and include a plan for how to counter threats on these platforms that adequately balances the need for action with the need to preserve privacy and free expression.

The United Kingdom's effort to construct a comprehensive framework for online safety will shape international norms on regulation. For these reasons, it is essential that it adopt an approach that balances safety with speech, and accountability with independence and innovation.

RECCOMENDATIONS

Lawmakers should reassess the "online harms" framework that underlies the White Paper. The Paper's scope for regulation – based on the concept of "online harms" – is ill-defined and overly broad. Conflating such a wide range of threats – across an even broader range of online platforms – could lead to regulatory overreach. The approach does not adequately account for the need for nuanced solutions that are tailored to both a specific threat and a particular platform. Policymakers should address:

- **Scope of harms.** The scope identified in the White Paper encompasses a broad range of threats under the framework of "online harms," including terrorist activity, disinformation, child sexual exploitation and abuse (CSEA), and cyberbullying. These threats pose very different challenges and demand substantially different legal and technical responses. While legislation and regulation is an appropriate response to some of the more well-defined of these "harms," like CSEA and terrorist content, applying the same framework to more nebulous threats like disinformation will threaten free expression.

- **Differentiation of response tactics. T**actics for combating these threats likewise vary. Different online platforms will need to employ different solutions. For example, while Facebook and Twitter can combat disinformation by targeting inauthentic behavior, YouTube (and its parent company, Google) should focus on ensuring that their algorithms promote trustworthy content. Conflating these challenges and platforms under one broad framework risks limiting nuance.

- **Barriers to competition.** Finally, the technical capabilities of large and established platforms, and the solutions that are suited to them, may not be directly transferable to smaller platforms. Exclusive focus on the needs and capabilities of larger platforms risks undermining the capacity of smaller ones to adhere to regulation, creating a harmful barrier to competition. In short, this tunnel vision risks cementing the very problems it seeks to address.

Recommendation: *Lawmakers should reassess the broad scope of the "online harms" framework and consider the different legislative actions that may be necessary (or unnecessary) to combat varied challenges. They should also acknowledge the need for solutions that are tailored not only to specific threats, but that account for the nature, size, and capabilities of online platforms.*

Lawmakers should reassess whether a government-established regulator is the most effective response to the wide range of challenges identified in the White Paper. They should also ensure that any such regulator is guided by a well-defined and proportionate enforcement structure and is endowed with credible independence from the government. They should examine three considerations in particular:

- **Applicability of the regulator.** Given the variance of challenges under the scope of the Paper – and the range of legal frameworks and solutions necessary to counter those threats – lawmakers should reassess whether empowering a single regulator under such a broad mandate is the appropriate response. While a regulator may be an effective means of exercising oversight of platforms' efforts to combat illegal content, charging it with the power to supervise vaguely defined "online harms" may restrict expression.

- **Proportionality of punitive measures**. If lawmakers proceed to establish an independent regulator, it will be important to establish a clear framework for penalties. If punishments are disproportionate or enforcement structures are nonspecific, platforms are likely to err on the side of restricting online discussion. In addition to degrading freedom of speech, that would play directly into the equivalence narratives of authoritarians. Narratives equating Western democracies with autocrats suppressing dissent may be especially potent in countries struggling to establish standards for the protection of speech, both online and off.

- **Independence from government**. Any regulator must have credible independence from the government. Lawmakers are crafting legislation for the United Kingdom, but they should be mindful of precedent. A less-independent regulator presents a substantial – though correctable – problem in a country with robust democratic institutions. In others, such a regulator may prove an insurmountable threat to free expression

Recommendation: *Lawmakers should reassess whether an independent regulator is an effective method to combat the full range of "online harms" encompassed in the White Paper and consider other actions for countering threats that are difficult to define. If lawmakers proceed to establish an independent regulator, they should ensure that it is guided by a defined and proportionate enforcement structure and that it maintains credible independence from government.*

Lawmakers cannot ignore "private communications." The Paper does not include decisive conclusions on how to define or regulate what it refers to as "private channels." Lawmakers must remedy this gap. Any regulatory structure that does not address private communications is incomplete and will not be effective at countering present threats to the information commons, never mind future ones. Specifically, lawmakers should consider:

- **The definition of "private communications."** In its current form, the Paper offers little related to combating threats that spread through these channels. Lawmakers should, in consultation with outside experts and industry professionals, establish an appropriate definition of private communications, which includes platforms that facilitate end-to-end encrypted communication, such as WhatsApp and Telegram.

- **A response for encrypted platforms.** If lawmakers restrict public platforms but do not regulate private communications, platform companies will shift conversations toward encrypted services where they can shed accountability. The "online harms" acknowledged in the Paper will not disappear on private platforms – many already flourish in such environments. Deconstructing the online public square would also have negative implications for democracy.

- **Specificity to protect privacy.** Vague or poorly designed legislation targeting private communications could pose a threat to personal privacy for citizens and set a dangerous precedent for less democratic governments.

Recommendation: *Lawmakers should construct a definition of "private communications" that includes encrypted messaging platforms and craft legislation that regulates "online harms" on these platforms without threatening democratic norms.*

CONCLUSION

By pioneering efforts to establish a comprehensive online safety regime, the U.K. government has shouldered a heavy responsibility for shaping international norms. This responsibility requires careful thought and action. Aspects of the U.K.'s approach are likely to be replicated around the world, including in countries with less stable democratic institutions. Authoritarian actors may manipulate regulatory rhetoric to justify the oppression of citizens. And developing countries – in which social media often plays a key role as a conduit to the Internet – may soon seek to establish their own norms for online safety.

To construct a more effective policy and support the integrity of democratic norms, lawmakers should reassess the "online harms" framework underlying the White Paper, and should acknowledge the need for solutions tailored to both specific threats and platforms. They should consider whether empowering a government regulator to oversee such a broad range of threats is an appropriate solution, and should ensure that any such regulator is both credibly independent from government and guided by a clear and proportionate enforcement structure. Further, lawmakers should define "private communications," and ensure that policies directed towards encrypted platforms balance safety with privacy.

Finally, lawmakers must remain vigilant of the global implications of their efforts, and when facing tradeoffs, do what is best for democracy.