GNI Submission to the Government of Vietnam on Potential New Decree 72 on the Management, Provision and Use of Internet Services and Online Information

I. Introduction

The Global Network Initiative (GNI) welcomes the opportunity to provide feedback on Vietnam's 'Draft Decree', to replace the Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information and Decree No. 27/2018/ND-CP that supplements it, recently published for comment.

GNI is a multistakeholder platform that brings together 91 prominent academics, civil society organizations, information and communications technology (ICT) companies, and investors from around the world. Members' collaboration is rooted in a shared commitment to the advancement of the GNI Principles on Freedom of Expression and Privacy, which are grounded in international human rights law and the UN Guiding Principles on Business and Human Rights (UNGPs).

GNI has been following the evolution of Internet regulation in Vietnam since 2012, when GNI published a statement concerning the prohibited acts of expression, data localisation and content monitoring obligations as set out in Articles 5, 24, and 25 of the former Decree No. 72/2013/ND-CP.

GNI acknowledges the important role that the governments can have in regulating the ICT sector to enhance due process, transparency, and accountability. However, without carefully considered approaches and narrowly-tailored requirements on content-related decision-making, content regulation can lead to censorship and privacy infringement.

In 2020, GNI led extensive multistakeholder consultations with its members and external stakeholders, including governments in a wide range of jurisdictions, and published a policy brief titled *Content Regulation and Human Rights: Analysis and Recommendations* ("Policy Brief"), which summarizes our comprehensive, proactive advice to governments seeking to regulate digital content. The brief uses international human rights standards to analyze more than 20 governmental initiatives that seek to address various forms of digital harm and sets out a range of observations and suggestions on how to regulate content in a manner that upholds and strengthens human rights. In this submission, informed by the Brief, we detail some of our

key concerns - including mandatory user ID verification, privacy risks associated with the storage of sensitive data, cross-border monitoring and takedown of content, and the scope of government's blocking powers.

II. Lack of Clarity Regarding Scope of Application

Throughout the draft legislation, GNI has observed a general lack of clarity on terms that define the scope of application of the decree. Article 2 establishes an excessively broad category of regulated entities which covers "domestic organizations, [and] individuals, foreign organizations, [and] individuals directly participating in or related to the management, provision, [and] use of Internet services, online information, online electronic games." This not only creates considerable confusion between the different entities covered by the law regarding its applicability, but under our analysed provisions in Chapter Three, the indistinct obligation on companies to trace and self-adjudicate content raises serious freedom of expression and privacy concerns. In addition, as noted in our Policy Brief, the law disproportionately applying to companies of varying sizes across various layers of the ICT sector creates "the potential for liability among companies that are not well positioned to effectively or proportionately address content."

In the ICT context, the location of the right service in the data stream and their particular regulation is a primary condition to fulfill the necessity principle. As a general rule, the further a particular service is away from the end-user, the less control it has over user-generated content. Therefore, the consequences of a regulation may differ significantly from one type of service to another. The Government of Vietnam must therefore ensure a duty of care and narrowly define the services that it targets to minimize regulation. It must recognize the impracticability of perfect enforcement, and afford an appropriate degree of flexibility to private services, especially start-ups and smaller entities, to avoid unintended impacts on the pluralism of consumer services.

III. Mandatory Identification Requirements

The Draft Decree includes an unprecedented mandate for identity verification of user accounts with a mobile phone number across both foreign and domestic regulated services under several provisions in Chapter Three. In particular, Articles 26-3(dd) and 30-2(a) in their current format require covered entities to collect and retain users' dates of birth, citizen identity numbers, and

passport numbers for a minimum 2 years, to be provided to competent State authorities upon request. Pursuant to Article 26-3 of Decree 53/2022/NĐ-CP on the implementation of the Cybersecurity Law (2018), which provides a strict data localisation requirement for both foreign and domestic internet and telecommunications services, it seems possible that this data would need to be stored locally in Vietnam. The collection and retention of this sensitive information by private platforms is unwise, unnecessary, and disproportionate.

Contrary to the Government of Vietnam's stated intention to tackle cybercrime, the collection and retention of such a volume of sensitive data by private companies will actually create cybersecurity and cybercrime risks by providing a tempting target for hackers and other unscrupulous actors. In addition, it is unclear how the draft provisions may be compatible with people's right to delete personal data regulated in the 2023 Personal Data Protection Decree, or which law will prevail in cases of inconsistency. Furthermore, to the extent these requirements apply to accounts of users who have dual-citizenship or residence (or who change citizenship or residence) in other countries, they will likely create conflicts of law with data protection regulations in those countries. At a time when governments around the world are working to minimize the amount of sensitive information collected by private companies in order to protect user data, the Draft Decree unfortunately moves in a contradictory direction by creating significant privacy risks.

From a freedom of expression perspective, numerous authoritative UN bodies have documented the importance of preserving the ability for people to express themselves anonymously, especially in contexts where unpopular but protected opinions could lead to significant social and/or legal harm. As a signatory to the International Covenant on Civil and Political Rights (ICCPR), the Government of Vietnam is bound to protect freedom of expression. To the extent that it determines that certain identifying information is necessary for the investigation and prosecution of cyber crimes, it can and should use the resources already available to it to obtain the minimum amount of information necessary on a case-by-case basis, in accordance with the human rights principle of necessity. Countries around the world have demonstrated their ability to successfully prosecute such crimes while protecting users' rights and without resorting to blanket personal data collection and retention.

IV. Proactive scanning of content

The draft legislation introduces a multi-pronged approach to content monitoring by granting State authorities sweeping powers to search and access user data and content on foreign and domestic regulated entities and social networks. Articles 26-3(m) and 38-14 create a backdoor access for the government to significant amounts of users' personal information, which goes beyond standardized lawful interception for cybersecurity solutions and generates serious security risks for individuals, especially amongst minority groups in Vietnam. The provisions are also inexact and open-ended in terms of the reach of scanning tools and the type of content that can be accessed by State agencies, providing insufficient guidance on adequate measures for companies to establish compliance.

GNI notes that people's right to privacy under the Draft Decree is already undermined by the ambiguity in the definition of *Private Information* under the General Provisions in Chapter 1. To top that, there are no necessary guarantees of confidentiality or limits for exercising state power under Article 24-7, which empowers an inexplicit group of "competent State management agencies" to have vast control over users' private information online. This can lead to a broad and arbitrary application of the law, potentially across jurisdictional boundaries, which would be in direct violation of Article 17 of the ICCPR. Moreover, the draft decree does not specify how the tools for search and scanning ought to interact with private communications and other services that are protected with end-to-end encryption. GNI has previously warned against the precarity and security implications of direct access arrangements, and expressed concerns about approaches that require invasive monitoring of users. If, despite our concerns, the government chooses to implement such measures, they must be authorized in publicly available, clear and easily accessible and understandable laws and accompanied by explicit transparency, oversight, and accountability measures. The law must ensure that any access to user data is disclosed to the subject in a timely manner if they are used in any civil, administrative or criminal proceedings, and allow them to pursue remedial measures against their privacy or security violations.

V. Overbroad Monitoring Obligations, 24 hour Takedown Notices and Government Blocking Powers

The proposed decree details a robust set of obligations on content removal for regulated entities under Articles 26, 27, 37 and 38. As framed, these provisions could pose serious risks for freedom of expression and privacy. These obligations cover moderation practices around a broad list of non-specific prohibitions under Article 5-1 of the draft decree and Article 8-1 of the

2018 Cybersecurity Law. For instance, “distorting history, denying revolutionary achievements”, “causing confusion among the citizens”, “defamation of the people’s administrative authorities”, and “insulting famous people or heroes” are some of the acts prohibited by the Cybersecurity Law, which are subject to abuse by overzealous authorities.

Under the proposed approach, domestic and foreign regulated entities providing cross-border information to end-users in Vietnam must proactively monitor and remove illegal content, services, and applications within a 24 hour window. Even this narrow timeframe for removal would be eliminated in cases where platforms are notified by the Ministry of Information and Communication (MIC) of content that raises national security concerns. As with requirements to collect and retain user data, requiring proactive monitoring by platforms will unnecessarily lead to privacy infringements and run counter to the global trend toward limiting the amount of information collected by platforms.

Additionally, requiring platforms to not only monitor but also adjudicate which content falls afoul of vague prohibited categories will incentivize companies to err on the side of removal, causing significantly more content to be restricted than is necessary to ensure effective compliance with the law. Notably, the draft decree exacerbates this concern by failing to include any provisions that would allow users to challenge or seek remedy for unwarranted content removal. As noted in the Policy Brief, such stringent timelines “effectively hinder the ability of ICT companies to prioritize resources and make nuanced, content and circumstance-specific determinations. These time limits may also make it difficult for the author to contest the allegation (i.e., issue a counter-notice) or seek injunctive relief or other remedy.”

Adding to these concerns, the law goes a step further under Article 37 clauses 6 and 7, according to which, aggregated information websites - i.e. websites that automatically reproduce news articles from media companies, most often under copyright licenses - must connect their monitoring system with the MIC’s, and be subject to inspection by “competent State management agencies.” This provides an inroad for the State’s direct involvement in their monitoring processes while circumventing conventional legal processes. Putting aside questions about whether such a system could function technically, if it did it would almost certainly result in impermissible violations of user privacy, cybersecurity standards, and third country data protection laws.

In the Policy Brief, GNI recommended instead that governments seek to address concerns around illegal content through “laws that focus more broadly on articulating standards for

appropriate content moderation based on traditional rule-of-law concepts, such as transparency regarding decision making, due process around content determinations, and remedy for impacted users, [which] will be both more narrowly and appropriately tailored and more likely to provide the flexibility needed to allow platforms to adjust to changing circumstances, norms, and technology."

GNI is also deeply concerned about the potential extraterritorial impacts of the decree's broad blocking requirements that include the strict removal of social network accounts, community groups and pages, and content channels that violate the law. Any non-compliance on the part of digital platforms "without legitimate reason" allows the government to suspend or block their operations under Article 26-5(b) and Article 38-6. Unfortunately, these create additional incentives for overcompliance by ICT companies. We therefore recommend that the government provide definitional clarity and detail on what qualifies as prohibited expression, in addition to refraining from the imposition of blanket, strict time limits for content removal.

VI. Conclusion

As it currently stands, the Draft Decree raises several concerns for GNI. The extremely expansive and unclear scope of application of the decree, as well as its provisions on mandatory user identification, overbroad categories of prohibited content, proactive monitoring obligations, 24-hour content takedown, and the government's ability to suspend digital services for non-compliance with blocking requirements could all individually and collectively have significant negative and avoidable consequences on freedom of expression and privacy. If enacted and implemented in its current form, the Draft Decree would be difficult to reconcile with Vietnam's international legal obligations, would likely create significant conflicts of law, and would create significant disincentives for platforms to consider or continue operating in the country. GNI therefore urges the Government of Vietnam to address these concerns by implementing significant revisions to ensure that the Decree is consistent with the principles of necessity and proportionality, protects freedom of expression, upholds data protection principles, and avoids creating arbitrary infringements on privacy. In order to ensure such a result, the Government should engage in further consultation with academia, civil society, and potentially impacted companies. As always, GNI stands ready to facilitate and support such engagement.