June 30, 2022

BSA COMMENTS ON DRAFT LAW ON ELECTRONIC TRANSACTIONS

Respectfully to: The Ministry of Information and Communication

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Ministry of Information and Communication (**MIC**) on the Draft Law on Electronic Transactions (**Draft Law**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow.

BSA commends the Government of Viet Nam on soliciting inputs from the private sector on the Draft Law, which proposes new regulations and requirements concerning digital signatures, digital identities, trusted services and electronic contracts. Notably, the Draft Law also proposes a new Chapter – Chapter VII on "Electronic Transaction System, Digital Foundation and Digital Services" – which seeks to regulate digital platforms.

BSA recognizes that enacting policies and regulations to ensure online responsibility and accountability is necessary for protecting consumers and engendering trust in the digital economy. However, not all digital service providers and platforms present the same risks or concerns to consumers and the digital economy. In particular, enterprise software companies, which provide Business-to-Business (**B2B**) services and interactions, do not present the same consumer risks as social media and e-commerce platforms, which typically interface directly with individual consumers and end-users. Such services may also have very different risk profiles, depending on a range of factors including the nature, purpose, size, and user base of these service. Reflecting these distinctions in policies and regulations would allow regulators to strike the right balance between ensuring online responsibility and accountability, while giving digital businesses sufficient freedom to grow and innovate.

Summary of BSA's recommendations

BSA recommends the following:

- Adopt a tailored and risk-based approach to regulating digital platforms;
- Exclude cloud computing and operating system platforms from consumer-facing obligations;

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

- Exclude foreign digital service providers from registration requirement in Article 54 as Article 55 already imposes registration requirements; and

- Clarify important terms and obligations in the Draft Law.

Adopt a tailored approach to regulating digital platforms

The Draft Law sets out general requirements and obligations for digital platforms in Chapter VII Sections 1 and 2. In Section 2, digital platforms and intermediary digital platforms are both broadly defined as providing the ability to "interact, transact, and provide services." Section 3, on the other hand, sets out specific obligations for various types of digital platforms and services, which include social networking platforms, online information search and data analysis platforms, digital content sharing platforms, online communication platforms, online advertising platforms, e-commerce trading floor platforms, electronic financial platforms, cloud computing platforms, operating system platforms, and online sharing cooperation economic platforms.[2]

Despite setting out the variety of digital platforms, it appears that there is little differentiation in the obligations that apply to each digital platform. Rather, additional obligations are layered in Section 4 due to the platform's size and influence. All of the digital platforms and services listed in Section 3 are subject to the general obligations set out in Sections 1 and 2, which include requirements to "ensure that the digital platform does not contain information and documents prohibited by law"[3] and to provide "tools and mechanisms for organizations and individuals to report issues related to infringing information content and quality of goods/services."[4] In addition to these obligations, these digital platforms will be subject to state management and supervision by the relevant Ministry.

This "one-size-fits-all" approach for the Draft Law's core obligations, which imposes the same requirements across all digital platforms and services, will create disproportionate burdens for many businesses. For example, the general obligations impose requirements for digital platforms to moderate content on their platforms and to respond to consumer rights request. However, not all digital platforms are able to view, access, or moderate specific items of content. Many B2B services providers and platforms do not offer content sharing services directly to consumers or the general public, and therefore may not have the technical ability to remove, edit, or curate user-generated content that may appear online. Such B2B service providers are often also contractually bound by their enterprise customers to respect the confidentiality of their customers' data and are prohibited from accessing or viewing such data on their platforms.

In this regard, as a general principle, BSA urges MIC to take a tailored approach and apply different and proportionate obligations and requirements to different categories of digital platforms, keeping in mind the specific conduct and risks that these obligations and requirements seek to address.

Exclude cloud computing and operating system platforms from specific consumer-facing obligations

The Draft Law imposes various consumer-facing obligations across digital platforms. General obligations include:

[2] Draft Law, Articles 62-71.

[3] Draft Law, Article 53.

[4] Draft Law, Article 57.

- Ensuring that the digital platform does not contain information and documents prohibited by law and complies with Vietnamese law on content management and information posted on digital platforms;[5]

- Ensuring that the digital platform does not "create conditions" for the dissemination of information and documents prohibited by law;[6]

- Providing tools and mechanisms for organizations and individuals to report "infringing activities";[7]

- Providing users with the ability to access data generated during users' operations on digital platforms, providing data generated from electronic transactions on digital platforms to state agencies, as well as providing "necessary support measures" to users when they want to transfer their data to another data processing platform.[8]

In the case of an "intermediary digital platform",[9] additional consumer-facing obligations include:

- Providing reports to MIC showing the process of handling infringing information on its digital platform based on user complaints;[10]

- Incorporating a solution or mechanism to "censor content posted by users", "prevent and remove content that violates the law at the request of the MIC and competent authorities", and "temporarily block or permanently lock accounts that regularly provide information that violates the law";[11]

- Building an internal complaint system and handling complaints from users "within 48 hours after receiving the request from the user". It is unclear if this means simply acknowledging a user complaint within 48-hours or needing to have it fully resolved. If the latter is intended, this is a strict timeline that would be difficult to meet, especially for smaller platforms. It is also not clear whether platforms would have the flexibility to take appropriate action to complaints based on the severity and impact on the user.[12]

In line with the previous recommendation to adopt a tailored and proportionate approach to regulating digital platforms, BSA strongly urges MIC to exclude enterprise cloud computing and operating system platforms from the above obligations. Furthermore, MIC should carefully analyze the appropriateness of each obligation in light of the technical capabilities of each class of digital platforms identified in Section 3.

For context, cloud computing services at enterprise level are focused on providing B2B services, which enable the operations of a wide range of organizations around the world, including small and medium enterprises and large companies, local and central governments, hospitals, schools, and

[5] Draft Law, Article 53(4)(b).

[6] Draft Law, Article 53(4)(c).

[7] Draft Law, Article 57(3)(a).

[8] Draft Law, Article 59.

[9] Per Article 53(2) of the Draft Law, an "intermediary digital platform" is defined as "a digital platform established and operated to provide an environment in cyberspace, online activities, allowing many parties to join together to interact, transact, provide services and products and goods to their partners, customers and users."

[10] Draft Law, Article 58(6)(a).

[11] Draft Law, Article 58(6)(d).

[12] Draft Law, Article 58(5)(c).

universities, and non-profit organizations. Similarly, operating systems provide the infrastructure for devices and applications to connect to the Internet, but are not content service providers, nor can they control content shared on the services they enable. Neither of these distinct types of services have a direct relationship with individual end-users or the ability to view and control content on the platforms they support.

In contrast to consumer-focused digital platforms, such as social networking and electronic commerce platforms, which are accessible and used by individual end-users, cloud computing and operating system platforms are used by businesses to improve operations and productivity, enhance product and service development, and increase opportunities for innovation. As a result, these platforms work closely with their enterprise customers but typically do not interact directly with the individual customers or end-users served by those organizations.

Consequently, cloud computing and operating system platforms are not well-placed to take on the obligations set out above because they have limited access to their enterprise customers' data, including individual consumer identities or contact details. According to the shared responsibility model, enterprise customers will have control over their data, not cloud service providers. For example, a cloud computing platform's access to and knowledge of such data is frequently limited by privacy and security controls built into enterprise products and enforced by contractual terms.

Furthermore, it is the enterprise customer, and not the platform itself, that typically has a direct relationship with the individual end-user. To subject cloud computing platforms to consumer-facing obligations would not only be technically and practically unfeasible, but it could also place them in breach of their contractual and other legal obligations. Similarly, it is the enterprise customer that decides how the services provided by the cloud computing platform will be used, including how personal information and content from end-users will be collected and processed. The cloud computing or operating system platform offering will have little to no visibility of the personal information or content generated by the individual end-users and is generally limited by contracts regarding how the platform can access, handle, and use that information.

Using as an example the obligation to moderate or take down infringing information in Draft Law, a cloud computing platform would be unable to directly implement the requirement to remove specific content. This is because the cloud computing platform does not have a direct relationship with individual users of its customers' services and would have to rely on its, enterprise customer to identify the individual end-user remove the illegal content. In many cases, the cloud computing platform may lack visibility into content stored by their customers because of privacy controls built into their services. If the enterprise customer fails to comply with a content removal request, the cloud computing platform's only recourse may be to terminate the service it provides to the enterprise customer, but it cannot remove specific content. This outcome could be a disproportionate response that could result in many other services and applications also being shut down, potentially affecting the continuity of important operations impacting large numbers of individual end-users.

BSA therefore recommends specifying, under Articles 69 (Cloud computing platforms) and 70 (Operating system platforms) of the Draft Law, that these platforms are excluded from the aforementioned consumer-facing obligations. In addition, the Draft Law should make clear that requests for removal or takedowns of infringing information, including from MIC or other government authorities, should be sent to the enterprise customer, as they are they are the entity in direct contact with the individual end-users responsible for the content.

Exclude foreign digital service providers from registration requirement in Article 54 as Article 55 already imposes registration requirements

Under Article 54 (Digital services and obligations of organizations and individuals providing digital services), providers of "digital services using their electronic transaction systems and digital platforms"

are required to register their electronic transaction systems and digital platforms with the MIC.[13] This obligation appears to apply to all digital service providers regardless of whether they are foreign or domestic. However, Article 55 (Responsibility for registration and notification of digital platform activities) already requires foreign digital service providers to register if they:

- Operate under the Vietnamese domain name (.vn);
- Use the Vietnamese language as their display language;
- Allow users to transact and pay in Vietnamese currency; or
- Have 500,000 or more visitors from Vietnam per month for six consecutive months.

Given that foreign digital service providers are already required to register under Article 55, we recommend expressly excluding foreign digital service providers from the obligations set out in Article 54. This would streamline the regime and allow foreign digital service providers to better understand and discharge their obligations.

Clarify Important Terms and Obligations in the Draft Law

Several important terms and obligations in the Draft Law are left unclear and could create unnecessary confusion. **BSA recommends that MIC make clear and provide further details to the following terms and obligations.**

Terms which are unclear

- **"Large" and "Dominant" digital platform:** A "large digital platform" is defined as "an intermediary digital platform with a large number of regular users, collecting and managing data of many individuals and organizations in Vietnam",[14] whereas a "dominant digital platform" is defined as a platform that "plays a particularly important role, contributing to the connection between service and goods providers to a large number of users in the territory of Vietnam."[15]
    - It is unclear what is the criteria for determining whether a platform plays an "important role" and what is considered to be a "large number" of users. It is also not clear whether the "users" refer to business users, consumers, or both. The above factors determine the scope of the provisions relating to large and dominant digital platforms, and their vagueness and subjectivity may lead to an unnecessarily broad scope and potentially capture services or platforms which do not necessarily exert market dominance.
    - **In this regard, in determining whether a platform is a "large" or "dominant" digital platform, BSA urges MIC BSA urges MIC to consult the industry and issue a set of criteria based on service platform types and other factors, such as number of active users on the platform. In the context of dominant digital platforms, MIC may wish to consider other indicators which create barriers to**

[13] Draft Law, Articles 52 and 54(2)(a).

[14] Draft Law, Article 72(1).

[15] Draft Law, Article 74(1).

entry, such as the existence of entry barriers because of same-side[16] or cross-side[17] network effects.

- **Infringing information:** "Infringing information" is defined as "information related to goods and services that violate the law; information that violates the prohibitions of the law on information technology; the law on network security."[18]

    - In the absence of illustrative examples, it is unclear what types of information may be considered "infringing information". Other jurisdictions similarly addressing illegal content on digital platforms have often provided examples of the illegal content that digital platforms are required to moderate or take down when in receipt of a lawful order.

    - It is important to draw a distinction between content that is illegal and content that is lawful but harmful. Regulating the latter type of content should sit with platforms that should be expected to have terms of use agreements that limit this type of content.

    - Illegal content should be clearly defined to provide clarity for both service providers and users. Where illegal content is identified, service providers should be notified so they are not responsible for determining the illegality of content in Viet Nam.

    - **BSA recommends that MIC specify and provide illustrative examples of the types of information that would be considered "infringing information" under Vietnamese law, so that digital platforms can better understand their obligations in this regard. For avoidance of doubt, notwithstanding this recommendation, BSA continues to urge MIC to exclude cloud computing and operating system platforms from such content moderation obligations, as they have little to no visibility of the personal information or content generated by the individual end-users.**

Obligations which are unclear

- **Six-month transparency reporting:** Every six months, an intermediary digital platform provider is required to send a report to the MIC showing the process of handling infringing information on the platform, requests from state agencies to remove infringing information, complaints from users regarding the goods and services provided on digital platforms, and the average number of regular users of the platform.[19]

    - BSA recognizes the necessity of transparency in the context of improving consumer protection. However, given the reference to "goods and services provided on digital platforms", it is not clear whether the reporting obligations are meant to apply to only intermediary digital platforms which facilitate transactions of goods and services, or

[16] Some digital platform services, such as social media services, exhibit same-side network effects on the user side, such that an increase in the number of users tends to increase the value of a platform to a given user. The presence of same-side network effects gives rise to a self-reinforcing feedback effect whereby a digital platform with many users can easily attract even more users, making the platform even more valuable and likely strengthening its market power.

[17] Platforms such as app marketplaces are subject to cross-side network effects, whereby an increase in the number of users on one side of a platform affects the value of the service to a given user on another side of the platform. These network effects operate in both directions for app marketplaces, creating a positive feedback loop, as more consumers using the app marketplace will likely attract more app developers, which is likely to attract more consumers and so on.

[18] Draft Law, Article 58(6)(a).

[19] Draft Law, Article 58.

all intermediary digital platforms, even those which only enable online communications/interactions and do not provide a platform for transactions of goods and services. **In this regard, BSA recommends that MIC specify that the reporting obligations are intended to apply to only intermediary digital platforms that facilitate transactions of goods and services.**

- **Relatedly, BSA also urges MIC to reduce the reporting frequency from once every six months to once every calendar year.** BSA is concerned that overly frequent reporting obligations may require businesses to divert limited resources away from improving their digital platforms, thus stymying the overall development of the digital ecosystem in Viet Nam.

- **<u>Risk assessment</u>:** The Draft Law requires large digital platforms to "identify, analyze, and evaluate systemic risks that arise from the functionality and use of its platform".[20] Various ambiguities arise in the context of this obligation.

  - *First*, the factors for assessing whether there are "systemic risks" are overly broad. For example, one factor is whether "the intentional exploitation and use of digital platforms may lead to foreseeable adverse effects related to the protection of the people's health and national security". This could refer to a broad range of matters, ranging from cyberbullying to privacy breaches, which do not necessarily relate to systemic risks.

  - **BSA recommends refraining from using broad, "catch-all" provisions such as this, as it generates significant regulatory uncertainty. Instead, MIC should first define "systemic risk" and provide a list of situations where systemic risks may occur or be more specific about the risks that should be included in any risk assessment, depending on the service type**

  - *Second*, the Draft Law does not specify if the expectations and requirements for the risk assessment will be differentiated based on service type of the digital platform. While cloud computing and operating system platforms do not present the same consumer risks as social media and e-commerce platforms, the key functions they play in a country's critical infrastructure means that they are in a better position to report impairments or stoppages of critical infrastructure assets. **BSA recommends setting out different risk assessment priorities for different types of digital platforms.**

- **<u>Codes of conduct and crisis-handling</u>:** The Draft Law requires large digital platforms to "cooperate with other digital platforms through codes of conduct and crisis handling mechanisms prescribed by law".[21] In other measures such as the Digital Services Act, crisis handling measures are voluntary to prevent them from being abused. The legislation should have a clear definition of what constitutes a crisis and provide clarity on how this will be addressed through the proposed codes of conduct. **BSA recommends making the following clear: 1) that crisis handling measures will be voluntary, 2) whether the relevant codes of conduct will be developed by MIC or by the digital platforms; and 3) the definition of what constitutes a crisis.**

[20] Draft Law, Article 73(1).

[21] Draft Law, Article 73(2).

- **<u>Compliance Supervisor</u>:** The Draft Law requires large digital platforms to appoint "one or more specialists in charge of monitoring the compliance process with the provisions of the digital platform's obligations." However, it does not specify if the compliance supervisor needs to be stationed in the country. **BSA recommends expressly allowing compliance supervisors to be stationed outside of Viet Nam, subject to an undertaking from the digital platform that the compliance supervisor can fully discharge his or her duties from abroad.**

- **<u>Recommendation Algorithm</u>:** Dominant digital platforms are obliged to provide their users with options to turn off the recommendation algorithm, to not set up recommendation algorithms that "prevent users from making accurate decisions when buying goods/services" and to inform and disclose to users the "principles, purposes and intentions, and key operating mechanisms" of the recommendation algorithm.[22] However, this obligation appears to be designed primarily for platforms that use recommendation algorithms to facilitate or encourage transactions of goods and services. Furthermore, the obligations are drafted in an overly subjective manner. It is not clear when a user has been prevented from making an "accurate decision" or "over-consumed" when purchasing goods and services, as purchasing habits and power vary widely between individuals. This subjectivity makes it difficult for businesses to adjust their practices to meet their obligations. As such, **BSA recommends: 1) excluding cloud computing and operating system platforms from this obligation, as they do not use recommendation algorithms to facilitate or encourage transactions of goods and services; and 2) deleting Article 74(2)(b), as it is too subjective and will lead to regulatory confusion.**

Conclusion

We hope that our comments will assist MIC as it considers regulations for digital platforms. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong

Tham Shen Hong
Manager, Policy – APAC

[22] Draft Law, Article 74(2).