10 August 2022

BSA COMMENTS ON SINGAPORE'S ONLINE SAFETY PUBLIC CONSULTATIONS

Submitted Electronically to the Ministry of Communications and Information

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Ministry of Communications and Information (**MCI**) on its public consultation regarding proposed measures to enhance online safety for Singapore-based users of social media services (**Consultation**).[2]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Many of BSA's member companies have made significant investments in Singapore, and we are proud that many Singaporean organisations and consumers continue to rely on our members' products and services to support Singapore's economy.

BSA recognises the prevalence of harmful online content and appreciates the pressing need to address the risks presented by such content. BSA has previously provided comments to Australia's Department of Infrastructure, Transport, Regional Development and Communications as part of their public consultations on the *Online Safety Act 2021* (**Online Safety Act**) and the associated *Online Safety (Basic Online Safety Expectations) Determination 2022* (**BOSE**).[3]

Summary of BSA's Recommendations

MCI has identified two proposed measures to address the risks of harmful online content: (1) a Code of Practice for Online Safety; and (2) a Content Code for Social Media Services (collectively, the **Codes**). In designing the Codes, BSA recommends the following:

---

[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, Kyndryl, 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.

[2] Public Consultation on Enhancing Online Safety for Users in Singapore, July 2022, https://www.reach.gov.sg/Participate/Public-Consultation/Ministry-of-Communications-and-Information/public-consultation-on-enhancing-online-safety-for-users-in-singapore.

[3] See:

a) BSA Response to the Online Safety Bill 2020 Consultation, February 2021, https://www.bsa.org/files/policy-filings/02122021ausonlinesafety.pdf;

b) BSA Submission to the Online Safety Bill 2021 Committee Inquiry, March 2021, https://www.bsa.org/files/policy-filings/03022021ausonlinesafetycmte.pdf;

c) BSA Comments on Basic Online Safety Expectations, November 2021, https://www.bsa.org/files/policy-filings/11122021bosecmts.pdf.

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

- *First*, adopt a narrow definition of "social media services" to ensure that obligations to proactively detect, moderate and take down harmful online content are applied to the services that pose the greatest risk of harm.

- *Second*, expressly exclude enterprise services, which are services designed primarily for enterprise customers or Business-to-Business (**B2B**) use, from the scope of the Codes.

Adopt a narrow definition of "social media services"

At the outset, BSA appreciates that the Consultation takes a risk-based approach to content regulation online, focusing on content available on social media services. As the Consultation notes, the risk of harmful content is greatest when it is "published on services that reach a wide audience" and "amplified" in a manner that promotes virality. The Consultation's narrow focus on "social media services" and the creation of Codes for "designated social media services"[4] is a sound approach as it rightly acknowledges that the obligations to proactively detect, moderate, and take down harmful online content should be carefully scoped and applied to the services that pose the greatest risk of harm.

In this regard, defining the class of services that will be subject to such obligations is critical. While the Consultation did not define social media services, the term "social media services" has been defined in other Singaporean legislation, most notably in the *Foreign Interference (Countermeasures) Act 2021* (**FICA**). FICA defines social media services as electronic services which (a) enable online interaction or linking between two or more end-users; **and** (b) allow end-users to post information or material on the service.[5]

We urge caution in using FICA's overinclusive definition of social media services and recommend that MCI adopt a definition that is better suited to the range of obligations contemplated by the Consultation. In contrast to FICA, the Codes are likely to impose requirements on companies that will necessitate the engineering of functionality into a service to enable proactive monitoring and removal of harmful content. While such requirements to proactively monitor and remove harmful content may be appropriate when applied to consumer-facing social media services, FICA's overinclusive definition of social media services may apply these same obligations to other service providers which present little risk of disseminating harmful online content and should not be designated as social media services.

In particular, FICA's definition may capture enterprise service providers which provide online services for business purposes – such as applications that enable messaging or voice communications between business collaborators or between a business and its customers, video-/voice-conferencing or other forms of online collaboration for business purposes – and which do not disseminate content to the public in a manner that is intended to amplify the reach of the content. A narrower definition would make clear that such online services used for business purposes are not social media services for purposes of the Codes. Indeed, the nature of such online services is to enable business interactions not social ones. They accordingly do not raise the same risks of distributing harmful online content that arise from social media services. For example, disseminating user-generated content to the public is a key common feature of many social media services as the dissemination to the public enables individuals to directly interact and communicate with other persons in the end-

[4] Consultation (2022), paras 10-23.

[5] Foreign Interference (Countermeasures) Act 2021, s. 13(1). "Social media services" means **(a)** an electronic service that satisfies all of the following characteristics: (i) the sole or primary purpose of the service is to enable online interaction or linking between 2 or more end-users (including enabling end-users to share content for social purposes); (ii) the service allows end-users to post information or material on the service; (iii) such other characteristics as are prescribed by the Regulations; or **(b)** an electronic service prescribed by Regulations as a social media service, but does not include a service which would otherwise be a social media service if none of the information or material on the service is accessible by, or delivered to, one or more end-users physically present in Singapore.

user's network or even the public-at-large. In contrast, online services for business purposes generally do not allow or provide for such public dissemination, nor do they amplify content in the same manner as social media services.

BSA has formulated an alternative definition for social media services for MCI's reference and consideration. This definition lists in greater detail what should be considered a social media service, thereby narrowing the scope of application to services that present the greatest risks of disseminating harmful online content.

"Social media service" means a publicly accessible, consumer-facing internet-based service or platform that:

(a) Has the primary purpose of facilitating social interactions between a potentially unlimited number of users of the service or platform;

(b) Uses algorithmic tools to recommend or otherwise promote content to users of the service or platform; and

(c) Allows users of the service or platform to do all of the following:

i. Create a profile for the purposes of signing into and using the service in a personalized manner.

ii. Post comments, information, ideas and other content that is visible to the public or to specified users, as determined by the platform users' preferences and privacy settings.

iii. Search for, and connect with, other platform users in order to view the content the user has posted on the platform.

iv. View and navigate a list of connections made by other users of the platform individuals within the system.

v. Visit a main feed or landing site where content from advertisers and connected users is automatically displayed.

Exclude enterprise services from the scopes of the Codes

If MCI prefers to use FICA's definition of social media services, BSA strongly recommends that MCI expressly exclude enterprise services from the scopes of the Codes.

Unlike social media services, which are provided directly to individual end-users, enterprise services are services designed primarily for enterprise customers or B2B use. These services are used by organisations of all sizes and across all industries to help them operate safely and efficiently, improve productivity, enhance product and service development, and increase opportunities for them to innovate and grow.

BSA members provide cloud-based tools and services to enterprise customers, including organisations in the healthcare, banking, energy, and defense industries. Given the sensitivity of their customers' data, enterprise service providers design their systems so that they have limited – if any – visibility into the data they are hosting and/or processing on behalf of their clients. Imposing a monitoring requirement on enterprise service providers would thus require them to reengineer their networks in ways that would create significant privacy and security concerns. It would, for instance, prevent enterprise service providers from offering user-controlled encryption protections that are critical to the security of sensitive data. Such an outcome could place service providers out of compliance with legal and contractual obligations, thus exposing them to potential liability.

Because of their limited access and oversight of the individual end-users' content, enterprise service providers are not capable of detecting, moderating, and taking down harmful online content. Requiring enterprise service providers to do so may require terminating the enterprise customer's account privileges completely, frequently a disproportionate response to addressing specific end-user content. Instead, the enterprise customer, with direct knowledge of individual customers and greater control over their content should be the entities required to address harmful content online.

The exclusion of enterprise service providers from obligations imposed on consumer-facing services is reflected in Singapore's *Protection from Online Falsehoods and Manipulation Act 2019* (**POFMA**). In POFMA, providers of "computing resource services" are not subject to the same onerous obligations as that of providers of consumer-facing "internet intermediary services".[6] For example, under Part 4 of the POFMA, only providers of internet intermediary and mass media services can be ordered to publish notices correcting a false statement on their platforms or to disable end-user access to the false statement.[7]

In the circumstances, BSA urges MCI to have express provisions in the Codes stating that services designed primarily for enterprise customers or B2B use are excluded from their scopes.

Conclusion

We hope that our comments will assist the Government as it moves forward with developing Codes to enhance online safety for Singapore-based users. 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

Manager, Policy – APAC

[6] Protection from Online Falsehoods and Manipulation Act 2019, s. 2(1). "Computing resource service" is defined as a service that provides the use of any computer hardware or software to enhance the processing capability or storage capacity of a computer (e.g., cloud computing and data centre services). "Internet intermediary service" is defined as services that: (a) allows end-users to access materials originating from third parties on or through the internet; (b) transmit such materials to end-users on or through the internet; or (c) displays, to an end-user who uses the service to make an online search, an index of search results, each of which links that end-user to content hosted or stored at a location which is separate from the location of the index of search results (e.g., social networking, search engine, content aggregation, internet-based messaging, and video-sharing services).

[7] Protection from Online Falsehoods and Manipulation Act 2019, s. 21-22.