12 February 2021

Online Safety Branch, Content Division

Department of Infrastructure, Transport, Regional Development and Communications

GPO Box 594

Submitted electronically

BSA RESPONSE TO THE ONLINE SAFETY BILL 2020 CONSULTATION

BSA | The Software Alliance (**BSA**) thanks the Department of Infrastructure, Transport, Regional Development and Communications for the opportunity to comment on the proposed Online Safety Bill 2020 (the **Bill**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members[1] are among the world's most innovative companies, creating software solutions and cloud services that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA supports the goal of the Australian Government to provide adequate protections to keep Australian consumers safe online. We commend the Australian eSafety Commissioner (the **Commissioner**) and the Office of the eSafety Commissioner (the **Office**) for the work they have conducted over the past 5 years in improving the online environment for Australians.

Recommendations

BSA recommends that the Australian Government:

1. Narrow the scope of covered entities subject to the Bill to exclude services designed for enterprise or business-to-business (**B2B**) use and not for consumers.

2. Change the requirement for removal of content by covered entities to "as soon as practicable".

3. Introduce an exemption from liability for entities that undertake actions in good faith to restrict access to or availability of material in line with the intent of the Bill.

[1] *BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.*

300 Beach Road
#25-08 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

Scope of Covered Entities

The Bill defines the entities covered by the Bill as social media services, relevant electronic services, and designated Internet services. In line with the approach taken by the European Union with the Terrorist Content Online Regulation and the proposed Digital Services Act (**DSA**)[2] BSA recommends that "electronic service", "relevant electronic service" and "designated internet service" be defined to apply only to consumer-facing services consistent with the purposes of the Bill.

Enterprise services — or B2B services — enable the operations of a wide range of organisations around the world, including small and medium enterprises and large companies; local and central governments; hospitals, schools, and universities; and non-profit organisations. Unlike consumer-focused services, enterprise services are not typically used by consumers, but instead by organisations of all sizes and across all industries to operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow.

Many enterprise service providers, including enterprise focused cloud service providers, have limited access to their customers' data, including individual consumer identities or contact details. Access and knowledge of such data is frequently limited by privacy and security controls built into enterprise products and enforced by contractual terms between the enterprise service providers and their enterprise customers. Therefore, the provisions of the Bill are applied most appropriately to the consumer facing businesses that deal directly with individual customers and disseminate information publicly and not the lower risk enterprise service providers.

BSA recommends that the definitions of "electronic service" and "relevant electronic service" in Section 5, and the definition of "designated internet service" in Section 14 be amended to explicitly exclude services designed for enterprise use and not by consumers.

Takedown period

The Bill proposes to require a covered entity to remove content within 24 hours of receiving a notice from the Office. BSA recommends instead that the requirement for removal of content by covered entities be changed to "as soon as practicable" in line with other harm-based schemes such as the Office of the Australian Information Commissioner's Notifiable Data Breach scheme.

Safe harbour for good faith voluntary takedown

In line with the intent of the Bill, covered entities should be incentivised to carry out voluntary self-initiated investigations or other activities aimed at detecting, identifying, and removing or disabling access to illegal content specified by the Basic Online Safety Expectations issued by the Minister or by other provisions in the Bill. If providers act in good faith to take down such content, they should be exempt from any liability that could arise from that action similar to the "Good Samaritan" provision in the proposed European Union DSA.

[redacted]

Yours faithfully,

[redacted]

Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance

[2] EU Digital Services Act; https://ec.europa.eu/info/sites/info/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf