17 November 2026

SUPPLEMENTARY SUBMISSION ON THE ONLINE SAFETY AMENDMENT (DIGITAL DUTY OF CARE) BILL 2026

Submitted Electronically to the Senate Environment and Communications Legislation Committee (the Committee)

The Business Software Alliance (**BSA**)[1] filed our principal submission on the Online Safety Amendment (Digital Duty of Care) Bill 2026 (**Bill**) on 30 October 2026.[2] This supplementary submission addresses recent proposals to incorporate a direct right of action into the Bill, such that individuals may directly sue a person responsible for an online service for breaching the Digital Duty of Care (**Duty**).

Our primary recommendation is unchanged. Business-to-business services should be excluded from the Duty, in line with a risk-based approach.[3] The Act's definitions are overly broad and reach well beyond consumer-facing services, capturing workplace collaboration tools, software-as-a-service applications of every kind and the cloud infrastructure on which customers store material. The result is that business-to-business services, which carry a fundamentally different risk profile from consumer technologies, sit squarely within the Duty. Furthermore, a business-to-business service provider usually has no direct relationship with individual customers of their business clients, and is subject to technical, legal, and contractual obligations that generally prohibit them from inspecting their enterprise customers' data except in limited circumstances. The Duty assumes that an entity that provides a service always has full visibility of end-user data and control over how the service is used, which is not the case for a business-to-business service provider. Consequently, the Duty binds providers who cannot discharge it, and reaches well beyond the harms it was designed to address.

---

[1] BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud services, collaboration systems, enterprise software and cybersecurity solutions, which many Australian companies and government agencies rely on.

BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] BSA Submission to the Senate Environment and Communications Legislation Committee on the Online Safety Amendment (Digital Duty of Care) Bill 2026, October 2026, https://www.bsa.org/files/policy-filings/10302026bsasenddoc.pdf.

[3] The Department of the Prime Minister and Cabinet's Legislation Handbook is instructive in this regard. See: https://www.pmc.gov.au/resources/legislation-handbook. As set out in Chapter 1 Section 1.21:
The following principles are to be applied by policy makers, instructing agencies and drafters when developing legislation:

a. *consider all implementation options—don't legislate if you don't have to;*
b. *when developing policy, reducing complexity and unnecessary regulation is a core consideration;*
c. *laws need be no more complex than is necessary to give effect to policy;*
d. *those affected by the legislation are able to understand how the law applies to them; and*
e. *continual assessment of the clarity of a proposed law is desirable—from policy development through to consideration by the Parliament (for Acts) or consideration by the rule-maker (for legislative instruments)*

In the absence of an express exclusion for business-to-business services in the Act, introducing a direct right of action could create significantly more concerns. As things stand, the Duty already exposes business-to-business service providers to liability even when they have no visibility of, or control over, the conduct complained of. This will be exacerbated if a direct right of action is introduced, as it encourages enforcement of the Duty by way of private litigation. For example, an employee who is harassed by a colleague over a workplace messaging tool could start proceedings of their own accord against the software vendor. Potential consequences are as follows:

- Intrusive compliance architecture being built into enterprise services and products;
- A flurry of litigation as the limits of the Duty are tested in the courts, including vexatious claims brought to pressure companies into settling;[4]
- A less certain enforcement environment for companies and less useful guidance to individuals;
- Reduced investment and innovation due to regulatory uncertainty; and
- Higher operating costs across the enterprise software market, ultimately borne by the Australian businesses and government agencies that rely on these products and services.

In view of the above, BSA: 1) reiterates the importance of an express exclusion for business-to-business services; and 2) cautions against the introduction of a direct right of action. BSA members supply the software, cloud and security services that all sectors of the economy depend on. They pose little risk to Australians online, contribute to their security and privacy, and are not in a position to discharge obligations designed for the platforms that do. If the Committee does not recommend an express exclusion for business-to-business services, and a direct right of action is nevertheless introduced, that right should at least be confined so that it does not extend to business-to-business providers.

We urge the Committee to take these considerations into account as it reports on the Bill. Thank you very much.

Yours sincerely,

Tham Shen Hong

Director, Policy – APAC

[4] BSA raised similar concerns with the Attorney-General's Department in 2023, when the Privacy Act Review Report proposed a direct right of action and a statutory tort for serious invasions of privacy. In our submission, we used the California Consumer Privacy Act (**CCPA**) as an example of "the flurry of litigation that could ensue" if a direct right of action was introduced. The CCPA gave consumers a direct right of action against businesses, individually or as a class. Despite that right being narrowly scoped, approximately 50 lawsuits invoking the CCPA were filed in the seven months after it took effect, and plaintiffs "challenged the limits of the CCPA's private right of action in every way they could". That included seeking to apply it retrospectively and beyond its geographic reach, disregarding the limits on which violations could support a claim, and using the CCPA as the standard of care in claims brought on other grounds. See: BSA Comments on the Privacy Act Review Report, April 2023, p. 10, https://www.bsa.org/files/policy-filings/04102023bsaaupriv.pdf.