



12 November 2021

Director, Online Safety Reform and Research Section
Department of Infrastructure, Transport, Regional Development and Communications

Submitted electronically

BSA Comments on the draft Online Safety (Basic Online Safety Expectations) Determination 2021

BSA | The Software Alliance (**BSA**) thanks the Department of Infrastructure, Transport, Regional Development and Communications (**Department**) for the opportunity to provide comments on the draft Online Safety (Basic Online Safety Expectations) Determination 2021 (**Determination**).

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

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members¹ are among the world's most innovative companies, creating enterprise software solutions and cloud services that spark the economy and improve modern life. Our companies are primarily in the business of providing business-to-business (**B2B**) services to organizations of all sizes and types (including small- and medium-sized enterprises) in many different sectors including for-profit businesses, non-profit organizations, and government entities.² Our members' products and services enable the operations of other organizations, helping them operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow.

In this context, we respectfully describe our concerns and recommendations regarding the following topics:

- **Considerations of risk** and other factors when determining the scope of applicability of specific Expectations and related obligations to **enterprise software services that typically present little risk of harm to Australian users, do not interact directly with "end-users", or are not primarily designed to disseminate content to the public.**

¹ BSA's members include Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zendesk, and Zoom.

² How Enterprise Software Empowers Businesses in a Data-Driven Economy at: <https://www.bsa.org/policy-filings/how-enterprise-software-empowers-businesses-in-a-data-driven-economy>

- **Application of the Expectations and related obligations** to enterprise customers with the proximate relationships to “end-users”.
- **The critical importance of encryption** as an effective data security and privacy related tool, especially for enterprise services that rely on the trust of their enterprise customers, including government customers.

Risk and the Scope of Covered Services

According to Section 13A of the Online Safety Act (**Act**), a “relevant electronic service” includes, among other things, a “chat service that enables end-users to communicate with other end-users”.³ Depending on how “chat service” is interpreted, it is possible this could include a wide variety of often ancillary functions frequently included in various enterprise software services designed to enhance productivity and communication among team members within and between organizations. The communications functions of such services are designed, and are typically used, to enable and enhance collaboration among colleagues for various business or professional purposes, including the conduct of government business, and are NOT typically designed, or used, to disseminate content to the public.

Some enterprise software services also facilitate communications between end-users of enterprise customers for a variety of purposes including for protecting the privacy of individual end-users, the customers of the enterprise customer. As an example, an enterprise service provider may provide a communication service to their enterprise customer that allows an employee of that enterprise customer to directly communicate with the enterprise customer’s individual customers (i.e., the “end-user”) in a manner that prevents both the individual customer/end-user and the employee from gaining access to contact information or other personal information of the other.

Because of how enterprise services are designed, how they are used, and by whom, they often present very little risk of exposing Australians or other individuals to harmful content.⁴ Therefore, it is important for the Determination to reflect a prioritization of the Expectations and related obligations that is based on online safety risk, as well as other functional considerations.

BSA is part of a coalition of industry associations working on the Industry Codes called for in Division 7 of the Act.⁵ In consultation with the Office of the Commissioner, and based on the Position Paper released in September,⁶ the coalition is working to consider how to incorporate a risk- and function-based approach to the development of the Industry Codes. This reflects the reality that not all online services present the same risk of exposing Australians to harmful content, and that greater and more specific obligations should apply to services that present a higher risk of harm.

The Industry Codes cover a broader spectrum of online industry service providers than the Determination.⁷ However, many of the considerations regarding the applicability of obligations to online services based on risk factors that industry and the Office are considering in the context of the Industry Codes should apply to the Expectations as well.

Risk is a function of multiple factors, including the type of online service (e.g., a software service that allows secure communications between the individual end-user customers of a third party enterprise customer, compared to a service designed to allow individual consumers/end-users to share content with the public), the intended use of the service (e.g., the service is designed for business or

³ Online Safety Act, Section 13A(1)(e)

⁴ We use the term “harmful content” to refer to the content and activities described in Section 11 and 12 of the Determination

⁵ Online Safety Act, Division 7 - Industry codes and industry standards

⁶ Development of industry codes under the Online Safety Act: Position Paper, September 2021 at <https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper>

⁷ Compare Online Safety Act, Section 135 (Sections of the online industry) with Section 45 (Basic online safety expectations)



professional application, compared to a service designed for use by the general public), the profile of typical users of the service (e.g., a service catering to specific groups of people, e.g. professionals, compared to a service that typically attracts members of the general public), the typical mode of use of the service (e.g., a service where most individual consumers/end-users use the service for professional purposes, compared to a service where users share a wide variety of content), and the actual content typically made available over the service (this might be some combination of the proportion of harmful content to total content as well as total volume of harmful content that is observed on the service, especially if that total volume is significant even if a small proportion of total content).

In addition, enterprise software service providers that design and offer such capabilities to enterprise customers, either in stand-alone fashion or embedded in a suite of software services, normally have very little visibility into, or control over, content shared over such capabilities. Enterprise software service providers also normally do not have direct interaction with, or knowledge of, individual consumers/end-users.

Recommendation

We recommend that the Determination explicitly acknowledge that what constitutes “reasonable steps”⁸ can and should differ, depending on the risk that the service will expose Australians to harmful content. In addition, the Determination should explicitly limit covered “relevant electronic services” to those services designed, or typically used, to disseminate content to the public and where the service providers have direct commercial relationships with individual consumer/end-users.

Application to Enterprise Customers

Many of the Expectations and related obligations of the Determination are tied to “end-users”.⁹ As mentioned above, enterprise software service providers offer enterprise software services to enterprise customers, and the enterprise customers then provide these services to their employees or individual consumers/end-users. As a result, the enterprise software service provider frequently has little or no direct relationship with such individuals.

It is therefore appropriate and important that the Expectations and related obligations are applied, at least in the first instance, to the enterprise customer and not to the enterprise software service provider. Making this clear will help individual end-users know to which organization they should raise concerns or file complaints and will streamline any inquiries by the Commissioner, focusing limited resources on the enterprises that are able to monitor or regulate content over the services. Only in circumstances where the enterprise customer, with the direct relationship with individual end-users, is unable or unwilling to meet the Expectations and related obligations should the enterprise software service providers become involved.

Recommendation

We recommend that the Determination state that the Expectations and related obligations apply, at least in the first instance, only to the enterprise customer which has the direct relationship with end-users.

Encryption

The employment of strong encryption to data, especially in the context of enterprise software services, such as cloud computing platforms, is vital to creating trust in on-line commercial and related activities. Enterprise software services, including services that enable user-to-user communications, may involve data that is highly sensitive for their enterprise customers. The data may be sensitive trade secret or other proprietary information, it may contain government information that must be

⁸ Section 6 of the Determination

⁹ See Sections 6, 7 (ref. Section 6), 8, 9, 11, 12, 13, 14, 15, 16, 18, and 19 (ref. Section 13) of the Determination



protected from unauthorized access, and it may contain personal information that must be protected pursuant to the privacy laws of many jurisdictions, including Australia's.

Encryption is a powerful and essential tool to protect data should it be accessed in an unauthorized manner, such as through a successful breach. Such data, if encrypted, would not be useful to the would-be hacker, and would therefore protect the enterprise customer and its individual customers from the worst consequences of a data breach.

In addition, enterprise software service providers also frequently encrypt their enterprise customers' data at the request or demand of their enterprise customers (which can include government agencies or critical infrastructure operators) to minimize the possibility that the enterprise software service provider itself may gain unauthorized access to the enterprise customers' data or internal communications. Again, this is especially important for enterprise customers managing highly sensitive data, such as government agencies and critical infrastructure operators, and therefore it is critical that measures to protect against the distribution of unlawful or harmful content are balanced against the important imperative to ensure that sensitive data is secure and protected against unauthorized access and use.

It is not clear what are the "reasonable steps" the Determination requires of enterprise service providers in respect of services that use encryption.¹⁰ The Frequently Asked Questions (FAQs)¹¹ provide some helpful guidance in this regard. For example, we are encouraged that the FAQ's clearly state the Basic Online Safety Expectations do not require enterprise service providers to monitor users' private communications. However, some of the examples of "reasonable" steps cited in the FAQs, such as "detecting misuse through behavioural, account or online signals..." may not be feasible or appropriate for many enterprise service providers, and would be better addressed by enterprise customers if they interact directly with individual end users.

These are extremely important considerations, as any requirements that limit the use or effectiveness of encryption to protect enterprise customers' data could have severe negative consequences to the development of a robust digital ecosystem in Australia. Such requirements would undermine trust in enterprise software services and create conflicts with the expectations and obligations of laws and policies designed to strengthen the privacy protections, cybersecurity capabilities, and resilience of enterprises, critical infrastructure operators, and government agencies that rely on such capabilities to secure their data.

Recommendation

We recommend that the Determination omit Section 8 and any expectation with respect to encryption. If the Department considers the Expectation in Section 8 is necessary, then we urge that enterprise services are explicitly excluded from the scope of this expectation and that in any case, the Determination itself should clearly state that "reasonable steps" will not require any restrictions on the use of encryption and/or the use of tools to monitor encrypted data by enterprise software service providers.

Conclusion

We thank again the Department for the opportunity to provide these comments and hope they are useful as you continue to develop and implement measures designed to achieve the important goal of creating a safer and more trusted on-line experience for Australians. We also hope that our concerns and recommendations will help inform what is a challenging, but extremely important, exercise to

¹⁰ Section 8 (Additional expectation—provider will take reasonable steps regarding encrypted services) of the Determination

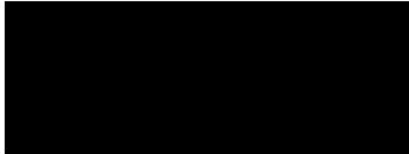
¹¹ Frequently Asked Questions: Basic Online Safety Expectations – October 2021 at <https://www.infrastructure.gov.au/sites/default/files/documents/frequently-asked-questions--basic-online-safety-expectations.pdf>



ensure that policies designed to reduce the availability of and exposure to harmful content online are appropriately targeted and do not inadvertently undermine other equally important considerations regarding data integrity, privacy, and security.

Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of any further assistance.

Sincerely,



Jared Ragland, Ph.D.
Senior Director, Policy – APAC



How Enterprise Software Empowers Businesses in a Data-Driven Economy

B2B software enables business customers to do what they do best—faster, smarter, and more efficiently.

Enterprise Software Supports Businesses' Operations

Enterprise software—or business-to-business (B2B) software—**enables** the operations of other companies. It helps organizations of all sizes and across all industries operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow.

The enterprise software industry supports a wide range of organizations across the world, including SMEs and large companies; local and central governments; hospitals, schools, and universities; and non-profits. By **offering trusted and responsible software solutions** to support their business clients' data-processing needs, enterprise software companies enable other organizations to service their own customers in turn.



Enterprise software optimizes the use of digital technology to support and improve business operations, empowering other companies to focus on what they do best, such as R&D and product design.



In Europe, almost **80 percent of large companies** and **35 percent of SMEs** use information-sharing software.¹

Enterprise Software Helps Businesses Benefit From Digital Transformation

Organizations in every sector of the economy increasingly rely on cutting-edge software to **run, facilitate, improve, and optimize their operations** every single day. Governments, public administrations, schools, and hospitals are also increasingly adopting these tools. Enterprise software underpins human resources and payroll operations; billing and financial transactions; research and development; product design; workforce collaboration, communication, and messaging; customer relations; and logistics and supply-chain management, among many other business services.



38 percent of small businesses in the **United States** cited increased sales and revenue as a benefit associated with using digital tools.²



Australian businesses are using more cloud than ever—**42 percent of businesses** across 2017–2018, up from 31 percent in 2015–2016.³



In times of crisis, such as the global outbreak of COVID-19, enterprise software tools help coordinate public health safety responses, maintain essential services, and support economic continuity.

ENTERPRISE (B2B) SOFTWARE PROVIDES CLIENT SOLUTIONS THAT:



Operate and Optimize Business Services

(including responsibly handling and moving information globally)



Protect and Secure Data and Business Information

(including providing strong, accountable privacy and security safeguards)



Innovate and Expand Beyond Existing Capabilities

(by using cognitive solutions such as analytics and artificial intelligence to better address customers' needs)

¹ EU DESI Index 2020, <https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi>.

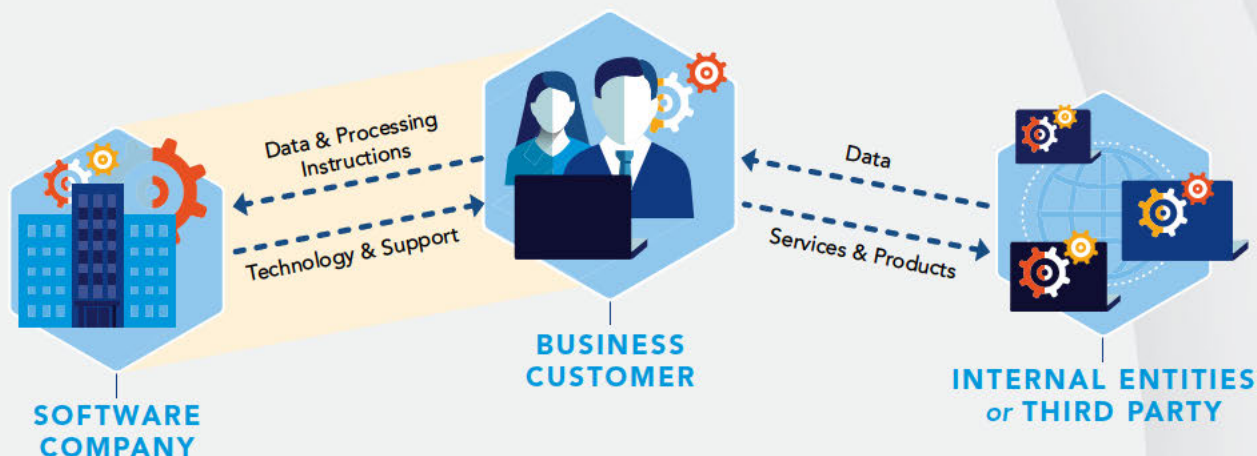
² <https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html>.

³ Characteristics of Australian Business, <https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2017-18>.

Enterprise Software Is Built on Transparency and Trust

Enterprise software companies and their business customers negotiate their relationship in contracts and licensing agreements to ensure they best address their clients' individual needs. **Enterprise software companies monetize their technologies and not the data of their customers.**

Enterprise software services, such as cloud computing, are used primarily for business-to-business purposes and are not consumer facing. **The business customers control their data and direct how it will be used.** Enterprise software companies do not have unfettered access to the data stored in their cloud infrastructure or service. Access and use of such data is reserved for the benefit and sole purpose of their customers.



Enterprise software companies operate under strong existing legislative requirements of data handling. Across the world, legal obligations often include accountability measures and technical safeguards that ensure enterprise software companies provide robust assurances of trust for their customers. Enterprise software companies also develop innovative, tailored, or customizable solutions for clients that are highly regulated, for example, in the health, financial, automotive, aeronautic, and telecom sectors and the semiconductor industry.⁴

➔ For instance, machine learning solutions can use data gathered across countries to create fraud detection systems in the financial sector.

Enterprise software helps reduce legal and operational risks for business customers who can be confident they are using tried and tested software products, with appropriate remedies and support, without having to develop their own software in-house. Enterprise software companies also often provide tools to facilitate their customers' compliance, for instance on privacy, consumer protection, cybersecurity, anti-money laundering, or energy efficiency.

⁴ See Cross-Border Data Flows: Enabling Local Economies and Driving E-Commerce, <https://www.globaldataalliance.org/downloads/WTOEventSummary20200702.pdf>.

How to Create a Successful, Responsible, Software-Enabled Economy



STRONG PRIVACY PROTECTIONS

Privacy is essential to building trust. Software-enabled business operations increasingly rely on data—and, in some cases, personal data—to function. As a result, data protection frameworks that create a user-centric approach to privacy must ensure the use of personal data is clear, transparent, and consistent with customers' expectations. Privacy laws should create robust obligations for all companies and organizations that handle individuals' personal data. This would ensure companies act responsibly while being able to pursue legitimate business interests.



CYBERSECURITY

Software innovation continues to connect people across the world. These online connections create efficiencies and spur economic growth, but they also create vulnerabilities that bad actors can exploit if the proper security measures are not in place. Addressing cybersecurity challenges requires innovative tools and practices to defend the integrity, confidentiality, and resilience of the connected ecosystem. One important tool is the ability to use the strongest available encryption technology when appropriate.



CROSS-BORDER DATA FLOWS

Cross-border data flows are necessary for companies to operate globally; leverage their resources and footprint across locations; innovate; and provide services to their customers, across sectors and geographies. For enterprise software companies and their business customers, the ability to transfer, and process, data globally is pivotal in ensuring the quality, reliability, security, personalization, and efficiency of service.



RISK-BASED AND TECHNOLOGY-NEUTRAL APPROACH

Software technologies evolve every day, pushing the boundaries of the benefits that technology can bring to organizations and people. Given the fast-paced nature of this industry and its adoption by customers, laws and regulations should strive to provide legal certainty, be outcome-based, and adopt a risk-based and technology-neutral approach, building on legal frameworks that already apply. Any new policy should set clear compliance goals and enable companies to adapt their practices and safeguards to the best-suited approach given their business model, the nature of their activity, their position in the value chain when contracted by others, and their risk profile vis-à-vis the established objective.



INTERNATIONAL CONVERGENCE

The value of the data-driven economy is in the ability of companies to operate across borders, reach new markets, and service customers regardless of location. Building on each region's own legal and cultural legacy, convergence of rules on privacy, cybersecurity, or data governance and compatibility of mechanisms play a critical role in growing cross-border business that increasingly rely on enterprise software around the world.