Friday June 24, 2022

To: George Cross
A/g Director, Data Security and Strategy, Technology Policy Branch
Digital and Technology Policy Division, Department of Home Affairs
By email: datasecurityandstrategy@homeaffairs.gov.au

Dear Mr. Cross,

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on the *National Data Security Action Plan Discussion Paper* (the Discussion Paper).

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, eBay, Google, Linktree, Meta, TikTok, Twitter, Snap and Yahoo, and its associate members are Change.org, Gofundme, ProductReview.com.au and Redbubble. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected. DIGI's members invest heavily in cyber and data security and the privacy of their users, through technical controls, user controls, strong accountability-based practices and policies.

Data security is integrated with privacy and cyber security

DIGI agrees with the Discussion Paper's assessment of data's central importance in a digital economy and a connected society. We also agree that laws need to be modernised to protect consumers and harness the benefits of a data-driven economy. This is why DIGI is also engaging in the reform of the Privacy Act, and we encourage the Department of Home Affairs to review our most recent submission in relation to the Attorney General's Department's reform proposals which we see as relevant to any Data Security Action Plan.

We also believe that cyber security is central to any data security action plans, and we would welcome further information than is provided in the Discussion Paper as to how the Data Security Action Plan differs from the work that the Department of Home Affairs is also undertaking in relation to the Australian Cyber Security Strategy. We would encourage your team to review DIGI's submission to the Department of Home Affairs' discussion paper *Strengthening Australia's cyber security regulations and incentives*, which we also consider extremely relevant to any action plans in relation to data security.

Close coordination on security and privacy is needed

There is a risk of duplication between these three processes, and other reforms pertaining to critical infrastructure, and we believe that closer coordination and integration of these strategies will further their goals and the data security of Australians.

DIGI welcomed the elevation of the cyber security portfolio to have an assigned Minister, as we have previously advocated for the reintroduction of this Ministerial position. To date, it has not always been clear where the responsibilities for Australians' cyber security lie across Government, as today responsibilities related to cyber security fall across the Australian Cyber Security Centre in the Australian Signals Directorate, the Attorney General's Department, the Office of the Australian Information Commissioner, the Australian Competition and Consumer Commission, the Office of the eSafety Commissioner, the Department of Communications and the Department of Home Affairs. Closer coordination across all relevant security, safety and privacy efforts is needed in order to ensure that plans are cohesive, an efficient use of resources, and conducive to evaluation.

Data localisation does not increase data security

DIGI is concerned to see the inclusion of data localisation in the Discussion Paper, which has not been contemplated in other privacy or cyber security reforms to our knowledge. This is because we reject the notion that data localisation increases data security, and we are concerned that it would have negative implications for the digital economy and the availability of digital services to Australians.

The free flow of information across geographic borders allows organisations to participate in the global economy, while data localisation requirements impede local operations, and increase the cost of doing business for organisations that operate across multiple jurisdictions. The physical location of data does not make it inherently more or less secure; what matters most are technological controls and policies to ensure security and privacy. Conversely, data localisation can make data more susceptible to attack, as a further centralisation within known data centres can make them a target for cyber attacks.

Furthermore, DIGI has observed that data localisation has been used in countries as a means to enable surveillance or censorship of citizens' online activities, and we are concerned that Australia's contemplation of local data storage requirements could set a troubling precedent that undermines the principles of an open internet, and emboldens proposals and surveillance activities in other countries.

Australia should work to align with international best practice in relation to data security and privacy, and it is worth noting that the OECD has long warned against the implications of data localisation, as they consider that: 'Suppliers should have the ability to supply services over the Internet on a cross-border and technologically neutral basis in a manner that promotes interoperability of services and technologies, where appropriate. Users should have the ability to access and generate lawful content and run applications of their choice'[1].

The regulatory environment impact our digital economy goals

The former Coalition Government's Digital Economy Strategy set out the vision for Australia to be a top 10 digital economy by 2030, a vision that DIGI supports wholeheartedly. This goal is ambitious, as Australia currently has the second smallest technology sector in the OECD[2]. However, it is achievable with *conscious* and *coordinated* efforts to improve the regulatory settings to build and grow technology companies in Australia, and to digitise the economy. Data security reform proposals need to be integrated within other strategies in relation to privacy and security, and also assessed for their implications on the Digital Economy Strategy, as part of a whole of Government approach.

DIGI looks forward to further engaging with the Department of Home Affairs' consultation processes in relation to data security and cyber security. Should you have any questions about the representations made in this submission, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director
Digital Industry Group Inc. (DIGI)

[1] Svantesson, D. (2020), *Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines*, OECD Digital Economy Papers, No. 301, OECD Publishing, Paris, http://dx.doi.org/10.1787/7fbaed62-en , p. 19
[2] AlphaBeta (2019), *Australia's Digital Opportunity*, accessed at https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf