Meta

9 June 2022

To whom it may concern,

Meta welcomes the opportunity to respond to the Department of Home Affairs' consultation on the National Data Security Action Plan.

It is essential for Australia to have the right framework in place for privacy, data and cyber security. The framework should enable the growth of the digital economy, facilitate cross-border trade and e-commerce, and minimise costs on businesses and consumers - while providing Australians with confidence about how their data is collected, managed and secured.

Achieving this environment is a collective responsibility. Governments, industry and individuals all have a shared interest in ensuring a strong security ecosystem in Australia, as a weakness or vulnerability at any point can impact the environment as a whole.

Meta recognises the importance of strong privacy, data and cyber security practices - our success is dependent on ensuring digital trust, and privacy and protecting data are at the heart of this. At a global level, we now have more than 40,000 people working on safety and security at Meta, and we've invested more than US$13 billion (~AU$18 billion) on safety and security since 2016, with more than US$5 billion (~AU$6.9 billion) invested in 2021.

Meta takes a multifaceted approach to data security - it is a complex and serious issue. It begins with privacy considerations, including how data is collected, used and stored. It extends to cyber security considerations, ensuring both data and critical infrastructure are protected from external threats and potential abuses.

To Meta, data security cannot be considered as an amalgamation of these different elements of the data lifecycle. Each step - whether it be privacy or cyber security - has different considerations and sensitivities, and requires different policies, tools, partnerships and infrastructure.

Meta has engaged with the Australian government extensively over the past few years on various proposals in this space. What has been clear across these consultations is that each of these policy areas have different sensitivities, technical considerations, interfaces with users, and outcomes they seek to achieve.

Many of the areas covered by the Data Security Action Plan have been covered in the Review of the Privacy Act 1988, led by the Attorney-General's Department, and the consultation process on cyber security regulation and incentives, led by the Home Affairs Department. Consultation on the Data Security Action Plan should consider Meta's comments as part of these processes, available in our responses to 'Strengthening

Australia's cyber security regulations and incentives',[1] and 'Privacy Act Review - Discussion Paper' for further detail.[2]

Given the ongoing, comprehensive reform agenda, an Action Plan risks duplication with existing processes. There is also a risk that the Action Plan introduces additional uncertainty for industry and consumers, and further time and cost burdens, particularly for small businesses, given the new comments about the need to localise data within Australia.

The Government should assess whether the proposal for the Action Plan aligns with best practice regulatory principles - namely, that it is necessary, fit for purpose and does not duplicate existing processes.

There is one significant issue raised in the Action Plan that is not contemplated by other reviews - local data storage. Data localisation requirements can inhibit business' growth - a 2015 study by Leviathan Security Group found that localisation requirements raise the cost of businesses (potential costs of hosting data as well) by 30-60 percent.[3]

Local data storage requirements also have broader implications for the state of an open, global internet. Personnel and data localisation measures such as those in India, Vietnam, Turkey and China, are often intended to facilitate the surveillance or censorship of citizens' online activities and violate individuals' human rights including freedom of speech, expression, access to information, and privacy and due process rights.

Australia's contemplation of local data storage requirements could set a concerning precedent that undermines the principles of an open internet and emboldens other countries with a different vision of the internet's future.

We encourage policymakers to ensure any proposals for further reform considers the broader geo-political context and state of the global internet, and encourages a liberal, open and democratic approach to the internet.

We welcome the chance to collaborate further with the Australian Government and broader industry on these issues.

Yours sincerely

Mia Garlick
Director of Public Policy, Australia, New Zealand & Pacific Islands

[1] Meta, '*Submission to Strengthening Australia's cyber security regulations and incentives*', September 2021, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives

[2] Meta, *'Submission to Privacy Act Review - Discussion Paper'*, January 2022, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/published_select_respondent?_b_index=180

[3] *See* Leviathan Security Group *Quantifying The Costs of Forced Localisation,* 2015, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf