DFAT Response to JSCOT Questions on Notice regarding the DEA

1. **What specific provisions or controls are contained in the agreement with respect to facial recognition technology?**

- The DEA does not contain specific provisions or controls with respect to facial recognition technology.
- The DEA does contain a provision on Artificial Intelligence (AI) that encourages cooperation on the development of ethical governance frameworks for the trusted, safe and responsible use of AI technologies.
- This provision encourages cooperation on AI, and sets in place a shared high-level intention to cooperate on the development of ethical governance frameworks for the trusted, safe and responsible use of AI technologies
- A framework for cooperation on AI is set out in the related MoU between the Department of Industry, Science, Energy and Resources (DISER), the Infocomm Media Development Authority (IMDA) and the Smart Nation and Digital Government Office.
- The DEA does not limit the Australian Government's ability to regulate AI, including on issues of privacy. None of the provisions in the DEA affect the ability of Australia to enforce regulations on privacy or require changes to Australian regulations, including the Privacy Act and the My Health Records Act.

2. **If this is to be regarded as a model for digital economy agreements, how does it differ from the European Union's 'general data protection regulation' (GDPR)?**
   Please provide a detailed list of the differences, and any relevant explanation for the variance in each case.
   Please address the proposition put by Monash Professor Norman Witzleb that the GDPR provisions create a higher privacy standard.

- The General Data Protection Regulation (GDPR) is a regulation in European Union law on data protection and privacy in the European Union and the European Economic Area.
- The Digital Economy Agreement is a bilateral trade agreement between Australia and Singapore. The DEA does not affect the ability of the Australian Government to enforce Australian privacy regulations or require any changes to Australian regulations, including the *Australian Privacy Act 1988*.
- Provisions that are negotiated in our FTAs (and digital economy agreements) do not impact on the operation of the Australian Privacy Act but instead demonstrate a joint commitment to ensuring appropriate privacy protections are in place domestically and to encourage interoperability of those protections and cooperation between countries.
- The Privacy Act continues to apply when personal information of Australians is transferred to another country (Privacy Principle 8).

DFAT Response to JSCOT Questions on Notice regarding the DEA

- The GDPR and the Australian Privacy Act share many similar protections:
  - Both laws foster transparent information handling practices and business accountability, to give individuals confidence that their privacy is being protected.
  - Both laws require businesses to implement measures that ensure compliance with a set of privacy principles, and both take a privacy by design approach to compliance.
  - Data breach notification is required in certain circumstances under the GDPR and under the Privacy Act.
  - Privacy impact assessments, mandated in certain circumstances under the GDPR, are expected in similar circumstances in Australia.
  - Both laws are technology neutral, which will preserve their relevance and applicability in a context of continually changing and emerging technologies.
- There are also some differences, including:
  - certain rights of individuals (such as the 'right to be forgotten') which do not have an equivalent right under the Australian Privacy Act;
  - the GDPR applies to data processing activities of businesses, regardless of size, that are data processors or controllers.
    - : the Australian Privacy Act applies to most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses.
- The OAIC's website provides a detailed comparison table of EU GDPR and the Australian Privacy Act: https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/
- The commitments in the DEA would not preclude companies from being able to meet EU standards through the GDPR, if they choose to comply with the EU regulation.

3. There is reference in the NIA to the capacity for countries to have access to the source code of software for investigation or enforcement actions, or to restrict cross-border transfer of information by electronic means where there is a legitimate public policy objective. Please provide examples of where this has occurred in relation to any such agreement or equivalent provision. If the source code is not provided on appropriate request, or if the cross-border transfer of information occurs in such circumstances what is the mechanism for requiring this to occur?

- Under the source code provision in the DEA, source code can be requested by a government agency, regulatory body or judicial authority for an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding.

DFAT Response to JSCOT Questions on Notice regarding the DEA

- An example of Australian legislation under which such requests can be made is the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA).
- The TOLA Act facilitates access to certain communications and data for the purposes of disrupting and investigating criminal activity and threats to national security, including organised crime and terrorism. The TOLA Act contains measures aimed at facilitating lawful access to communications and data through two avenues – decryption of encrypted technologies and access to communications and data at points where they are not encrypted.
- The TOLA Act stipulates conditions and penalties whereby a person commits an offence under the Act. Non-compliance with appropriate requests for source code under other laws and regulations would be dealt with according to those laws and regulations.
- The DEA, and provisions of the Singapore-Australia Free Trade Agreement (SAFTA) more broadly, specifically preserve Australia's ability to regulate key areas of public interest including privacy. The DEA also includes exceptions for essential security reasons, prudential reasons and for government information and government procurement.
- With respect to the cross-border transfer of information by electronic means, these exceptions are further boosted by explicit exceptions for legitimate public policy objectives.
- Legitimate Public Policy Objectives would encompass a range of possibilities regarding the adoption and maintenance of measures. Although the subject of specific exceptions in the DEA, we consider that certain data localisation requirements and restrictions on cross-border transfers of information, including for financial market infrastructure, for the treatment of credit information under the Privacy Act and under the My Health Records Act, are examples of legitimate public policy objectives.

4. In relation to the requirement under the A-SDEA for each party to maintain appropriate consumer protection laws, has an assessment and judgement been made in relation to the adequacy of Singapore's laws? Please provide details of the relevant law, with examples of provisions that match equivalent Australian provisions.

- Australia and Singapore have similar consumer protection systems.
- Both Australia and Singapore recognise the importance of adopting and maintaining transparent and effective measures to protect consumers from misleading and deceptive commercial activities, unfair contract terms and unconscionable conduct when they engage in electronic commerce.
- In Australia, the relevant legislation is the Australian Consumer Law (ACL) and the Competition and Consumer Act 2010.

DFAT Response to JSCOT Questions on Notice regarding the DEA

- In Singapore, the relevant legislation is the Consumer Protection (Fair Trading) Act (Cap. 52A).
- Both Australian and Singaporean legislation address:
  - unfair practices for a trader, in relation to a consumer transaction;
    - : including in relation to misleading and deceptive conduct; and
  - penalties, enforcement powers and consumer redress options.

5. Can you confirm that the deregulatory effect of the DEA which means companies operating services or platforms in Australia from Singapore can keep private their source code does not extend to algorithms?

- The commitments contained in the DEA do not change any existing Australian laws and regulations.
- The source code provision in the DEA contains a commitment for Parties not to require access to, or transfer of, software source code as a condition for the import, distribution, sale or use of software.
- The source code provision does not prevent source code being requested by a government agency, regulatory body or judicial authority for an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding.
- Source code could implicitly include algorithms, to the extent that algorithms are expressed in that source code.
- The source code provision in the DEA commits Australia to apply this rule to algorithms expressed in source code only if Australia makes such a commitment in another international agreement (or an amendment thereto) which enters into force after the DEA.

6. Please provide the details of, and summarised content/conclusions from the analysis of the potential tax revenue impacts of the A-SDEA.

- The Digital Economy Agreement does not impose any restrictions on the Australian Government's ability to enforce tax laws or develop new taxation regulation beyond existing obligations under the WTO.
- The Digital Economy Agreement also does not affect Australia's rights and obligations under any tax convention that Australia and Singapore are party to, including any OECD tax convention.