The Dialogue™

INFORM ENGAGE IDEATE

12TH APRIL 2022

BILATERAL DISCUSSION BETWEEN AUSTRALIA AND INDIA ON DATA PROTECTION REGIMES

REPORT

DRAFTED BY: KAMESH SHEKAR

Note: This bilateral discussion happened before the Personal Data Protection Bill 2019 was withdrawn from the Indian parliament.

TABLE OF CONTENTS

INTRODUCTION

The Dialogue (a Delhi-based think tank) organised a bilateral discussion between Australia and India on data protection regimes on 12th April 2022. For this discussion, we were delighted to host **Ms Angelene Falk, Australian Information Commissioner and Privacy Commissioner; Dr Amar Patnaik, Member of Joint Parliamentary Committee on Personal Data Protection Bill, 2019; Rahul Matthan, Partner, Trilegal.**

As India is at the cusp of enacting its data protection regime, the speakers exchanged notes on the data protection regimes in India and Australia through this discussion. The key focus of the discussion was to learn about implementational strategies followed by Australia under its data protection regime, where a single office tackles both the right to privacy and access to government-held information. The comparison was undertaken to assess possible solutions to friction points within India's data protection framework. However, the panel was mindful of the two jurisdictions' distinctive legal, administrative, and industry infrastructure and capacities. The broad themes discussed by the panellists are summarised below.

This discussion followed Chatham house rules; therefore, the views and observations have been summarised and not attributed to any speakers in this report.

THE AUSTRALIAN DATA PROTECTION REGIME

The panellists discussed the historical landscape of Australia's data protection regime and the functional and structural pillars of Australia's data protection authority.

HISTORY OF THE AUSTRALIAN DATA PROTECTION REGIME

The panellists noted a long history of the reform of privacy laws in Australia, commencing in 1988, where they applied only to federal government agencies, as opposed to the current laws that also regulate the private sector. Over time, bodies such as credit reporting bodies were included within the scope of regulation, and by 2001 the Privacy Act 1988 (Cth) (Privacy Act), covered the private sector. Australia is currently undertaking a review of the Privacy Act.

The Australia Information and Privacy Commissioner, supported by the Office of the Australian Information Commissioner (OAIC), is the independent statutory regulator of the Privacy Act and enforces compliance with the Act. It was brought to the panel's notice that the OAIC receives a statement of expectations from the Attorney-General, which sets out the government's expectations about government policies and objectives relevant to a statutory authority at a high level. The OAIC is expected to take a contemporary evidence-based, and proportionate approach to its regulatory role in promoting and upholding Australia's privacy and freedom of information laws.

STRUCTURE OF OAIC

The OAIC reports to the responsible government minister, the Attorney-General, through the annual report tabled at the Federal Parliament. Also, it tables a corporate plan every year that sets out its strategic priorities, its regulatory focus, and how the office will deliver value for Australia. In addition, the panellist highlighted that the Australian Information and Privacy Commissioner is required to appear three times a year before a Senate Committee, comprising representatives from a range of political parties, to answer questions about the office's performance and the expenditure of public funds.

The OAIC enforces the Privacy Act, covering personal information (including sensitive information, credit reporting and tax file number information), Australian government agencies, and the private sector (subject to an exemption for small businesses). The OAIC is separate from data protection authorities at the state and territory level, who is responsible for overseeing the handling of personal information by state and territory government agencies.

Besides, administratively, the panellist mentioned that the OAIC's privacy structure is across three main areas - (a) the regulation and strategy area, which is the proactive policy and advice arm of the agency, (b) the dispute resolution area that handles regulatory complaint, review and enforcement activities, and (c) education and awareness, including the corporate governance engine of the agency.

FUNCTIONS OF OAIC

The panellist highlighted that Australia's data protection approach had recognised a decrease in trust in private entities' handling of personal information and a need to restore citizens' confidence in how their personal information is handled. They also emphasised that good privacy practices can be an enabler of innovation in modern government services and go hand-in-hand with ensuring the country's sovereignty, security, individual choice, control and autonomy. The two primary purposes of the OAIC that panellists highlighted are to (a) uphold the right to privacy in accordance with the Privacy Act and associated privacy laws and (b) oversee information access rights per the freedom of information laws. The OAIC's active functions and powers, broadly sketched by the panellists during the discussion, include:

- **Guidance and monitoring obligations**

  There are proactive powers that allow the OAIC to provide guidance and advice to (i) regulated entities on how to comply with the law and (ii) the government on proposed laws, any impacts that they may have on the privacy of individuals, and how those impacts may be eliminated or minimised. In this way, panellists noted that the agency has the opportunity to influence the privacy landscape and embed good privacy practices across Australia.

- **Enforcement and adjudicatory function**

  Panellists mentioned that the OAIC accepts complaints from individuals about how organisations or government agencies covered by the legislation handle their personal information. At the same time, they noted that the Commissioner could initiate an investigation of her own accord in relation to any acts or practices that interfere with the privacy of individuals. Also, they added that the OAIC could take proactive assessments to identify risks within regulated entities and make recommendations on how those risks can be mitigated and prevented.

- **Education and awareness function**

  Through this function, the panellist mentioned that the OAIC seeks to ensure voluntary compliance with the law and avoid using regulatory powers unless required.

COMPARISON OF DATA PROTECTION REGIMES: AUSTRALIA AND INDIA

As the discussion revealed, the upcoming Indian data protection regime might incorporate several critical factors that have been modelled upon the Australian data protection regime. However, the panel highlighted the differences in the data protection regimes in Australia and India as tabulated below:

Table 1: Comparison between Australia and India Data Protection Regime

Australian Model	Indian Model	Inferences for India
Australia has one individual regulator charged with regulating two fundamental rights - the right to access government-held information and the right to privacy.	The Indian regulatory model has different regulatory bodies for both the right to privacy (envisioned DPA) and information.	The panellists observed that the Australian model may be beneficial for India, and some consideration and exploration must be done to understand the nuances of such a model.
Australia has some state and territory-level data protection authorities alongside the federal data protection authority.	There is no provision for establishing state-level authorities within India's upcoming data protection regime.	The discussion shed light on the need for state-level data protection authorities in India instead of a central-level data protection authority. The panellists highlighted that having one regulatory body take care of the rights of over a billion individuals may bring forth several potential implementation challenges.
Australian data protection laws primarily deal with personal information.	The Joint Parliamentary Committee's Data Protection Bill, 2021 includes personal data and non-personal data, which will be regulated by one data protection authority.	As the discussion revealed, having a data protection authority regulate both personal and non-personal data could avoid potential disagreements between different authorities, avoid confusion while classifying data and enable seamless interaction between the two verticals enmeshed within the same authority. However, some panellists pointed out that the personal data regulation is fundamentally a restrictive regulation that prevents one from doing specific actions with personal data. Whereas non-personal data regulation is fundamentally an enabling regulation. A panellist stated that the entire push of the non-personal data framework is to unlock otherwise locked information; therefore, bringing non-personal data under a single regulator may prove to be challenging.
The Australian data protection regime does not provide for a blanket data localisation law. However, there are several areas where the data localisation requirements are in place, e.g., Australian digital health records, and credit	India's data protection regime will include a data localisation framework which confines specific kinds of data transfers by imposing domestic storage and processing mandates.	As long as the data localisation laws comply with the normative principles of data protection, panellists mentioned that countries should be allowed to meet their national priorities and create exceptions to the free flow of data

information. In order for personal information to be transferred outside of Australia, the entity transferring data must take reasonable steps to ensure that the overseas recipient does not breach Australian privacy laws. Alternatively, personal information may be transferred overseas if the recipient's jurisdiction has a comprehensive data protection framework that protects personal information in a similar way to Australian privacy laws.	The Indian regulatory model has different regulatory bodies for both the right to privacy (envisioned DPA) and information.	across borders.
Some aspects of the Australian data protection regime coordinate with different regulatory bodies in different areas, given the need for complementary expertise.	India's data protection bill discusses the Data Protection Authority's coordination with other sectoral regulators.	Panellists pointed out that various sectoral regulators in India currently oversee privacy regulation in certain specific sectors. For Instance, the Reserve Bank India (RBI), looks after the privacy regulations concerning banking regulations, the Competition Commission of India (CCI), believes that privacy is a non-price factor for competition. Therefore, they suggest that India infer from the Australian model for sectoral cooperation and collaboration.

CONGRUENCE IN USAGE OF CONSENT MANAGERS IN INDIA AND AUSTRALIA

During the discussion, a panellist brought up India's consideration of incorporating 'consent managers' within its potential data protection regime. Within the Bill, lawmakers have inserted an institutional mechanism called the consent managers, which are independent entities responsible for managing data principals' consent for data sharing via an interoperable, secure, and transparent platform. "Account aggregators' earlier notified by the RBI that facilitate the consented transfer of financial data between regulated financial entities are the first in kind of consent managers. Panellists highlighted those intermediaries managing consent flows ensure greater privacy and may be designed to scale to meet the requirements of a diverse population.

The Australian data protection regime does not have 'consent managers'. However, panellists pointed out that Australia's consumer data rights framework includes 'consumer dashboards' where individuals may see and manage all of their consents for the collection and use of their data within the framework. The discussion also noted that a proposal had been put forward to the Australian government for an online privacy code which would, amongst other things, set out stricter notice and consent requirements for certain online platforms, particularly in relation to children and vulnerable groups. But the panel acknowledged that laws would need to be tailored according to each country's circumstances; the same devices cannot be plugged similarly, and appropriate adaptations are required.

WAY FORWARD

The panellists recognised that technology is moving exponentially and would require lawmakers to pay special attention to the potential effects and adversity this may have on global privacy. The panellist discussed some way forward pointers to be considered to have a successful and robust data protection regime for India as follows:

- **Proactive not reactive**

  Proactive privacy obligations must be incorporated for entities to be accountable upfront for handling personal information. Panellists emphasised that authorities must promote that 'privacy by design' is embedded into systems and processes. Besides, authorities must also ensure personal information is handled responsibly throughout the economy, including by the government.

- **Robust enforcement tools**

  As identified in the panel discussion, there must be a contemporary approach to regulation with a comprehensive regulatory toolkit. This includes individual complaints, suo moto initiative powers, the ability to enforce fines against entities breaching the law and taking action through the courts. Panellists pointed out that some data protection authorities only have recommendatory powers, and they are limited in their ability to shift the behaviour of regulated entities.

  Importantly, panellists emphasised the need for the capacity within the regulator to perform these functions. Staff needs to be equipped with legal skills and the ability to regulate emerging technologies and interrogate complex data information flows.

- **Diversifying financial portfolio**

  Panellists highlighted that in the UK, the Information Commissioner's Office is supported by a levy where all entities that handle personal information must pay a certain amount of money to the regulator to ensure they are appropriately resourced. A similar recommendation has been made to the Australian Government for consideration that would ensure a more substantial resourcing base for the OAIC.

- **Co-regulation**

  Panellists emphasised the need for collaborative regulation in ensuring the efficient and effective implementation of laws. Australia recently constituted a forum of digital platform regulators that includes authorities in Australia that regulate digital platforms, including the OAIC, the competition regulator, the e-safety regulator, and the communications regulator. This forms a collective of diverse regulatory perspectives. This also enables a one-stop-shop for government policymakers to engage with regulators on issues pertaining to digital platforms, ensuring consistency in digital regulation.

- **Global collaboration**

  Panellists discussed the need for global collaboration by discussing the Australian approach. The OAIC has a strong engagement with the Global Privacy Assembly, where it is a member of a number of working groups that provide leadership standards of data protection globally and promote consistent implementation of privacy principles for the good of global citizens.

Therefore, panellists highlighted that inferences from the Australian data protection regime and its growing jurisprudence could greatly be important in drafting India's upcoming data protection regime. They also emphasised that India would benefit greatly by focusing on the conceptual framing of its forthcoming data protection regime, not just from the perspective of framing laws and regulations for compliance purposes but also by building technological infrastructure that embeds some of the above-discussed elements and principles into its architecture.

The Dialogue™

INFORM ENGAGE IDEATE

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

https://thedialogue.co