# DATA BEYOND BORDERS: OTT PLATFORMS, THE DPDP ACT AND CROSS-BORDER DATA TRANSFERS

Anshika Singh, Jindal Global Law School


## ABSTRACT

The introduction of the Digital Personal Data Protection Act, 2023[1] ("DPDP Act") has been an important change in the Indian data governance system, especially regarding cross-border data transfers. Departing from previous proposals which mandate rigid data localization, the Act follows a much lenient, 'negative list' approach that permits the transfer of personal data out of India except to the jurisdictions identified by the Central Government.[2] The implications of this approach are far-reaching to Over-the-Top ("OTT") platforms, whose operating architecture, relies on constant transnational flows of data as the means of content delivery, algorithmic personalization, and the world-digital cloud-based infrastructure. This paper is a critical study which looks at whether the DPDP Act provides a coherent and adequate regulatory framework on cross-border transfer of personal data in OTT platforms. It goes on to examine Section 16[3] and its design on a statutory level, the accountability requirements of Section 8[4] and the relationship with sectoral regulations. It also goes on to compare the framework with constitutional principles of privacy and proportionality as enshrined in *Justice K.S. Puttaswamy v Union of India*[5] and also providing a comparative analysis to European Union's General Data Protection Regulation [6]("GDPR"). It ultimately finds that while the DPDP Act is logical in its economic and regulation goals, it is not enough to provide strong data protection as there are no systematic protection measures and so, the DPDP framework needs additional rulemaking and institutional development in order to be useful in governing the cross-border data flows in a globalized digital economy.


[1] The Digital Personal Data Protection Act 2023

[2] Taxmann, 'Cross-Border Data Transfers under the DPDP Act 2023' (*Taxmann*, 4 May 2025) < https://www.taxmann.com/post/blog/cross-border-data-transfers-under-the-dpdp-act/> accessed 23 March 2026.

[3] Ibid. s 16

[4] Ibid. s 8

[5] Justice K.S. Puttaswamy (Retd) and Anr v. Union of India and Ors AIR [2017] Supreme Court 4161

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

## Introduction:

The advent of OTT platforms has completely revolutionized the Indian media and entertainment industry structure. Digital companies such as Netflix, Amazon Prime Video, and Disney Plus Hotstar have completely transformed the way people consume content by providing on-demand, customized, and integrated global content. In contrast to conventional models of broadcasting, OTT requires extensive use of data-intensive technologies for filtration of content, optimization of user interaction, and monetization.

The main aspect of this transformation is the process of collecting, processing, and transferring of personal information across jurisdictions. OTT platforms frequently transfer cross-border user data to store, analyze, and use in machine learning. Such transnational data flows present serious legal and regulation issues especially in regards to protection of privacy, control across jurisdictions, and overall enforcement.

India's approach towards the regulation of such data streams has changed significantly in the last ten years. The proposed legislations that have been made earlier such as the Personal Data Protection Bill, 2019[7] and subsequent proposals, prioritized data localisation as a tool of data sovereignty. Nonetheless, concerns about economic efficiency, innovation, and global interoperability has come to the point where it has reconsidered its approach. The passing of the DPDP Act 2023 has showcased the recent transition to a more flexible regulatory structure which allows for cross-border data transfers to happen with limited restrictions.

This paper explores whether the DPDP Act provides a reasonable and adequate regulatory framework in the context of cross-border data transfer, specifically looking at OTT platforms. It examines the legal framework of the Act and the manner in which they apply to OTT-specific data practices and contrasts the Indian framework with its international counterparts, finally arguing that the DPDP Act is internally consistent in its design, but falls short when it comes to addressing the challenges of transnational data flows.

## OTT Data Practices and Cross-Border Data Flows:

OTT platforms have an underlying data-intensive structure, where personal information is both

[7] 'Personal Data Protection Bill 2019' (PRS). https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 accessed 23 March 2026.

an operational input and a strategic resource. These sites gather various types of data, such as personal identifiers, device data, IP address, location data, and a detailed behavioral data related to user preferences and viewing behaviors. This information is then applied to facilitate customized suggestions, optimization of streaming quality, and enhanced user interaction. The transnational character of data infrastructure of OTT services is a characteristic trait of these platforms. Here, their operations are based on distributed cloud computing networks and content delivery networks ("**CDNs**") that store and process data across a variety of jurisdictions.[8] As an example, data generated in India could be processed in data centers in the United States or Europe, whereas content delivery could be supported by the use of servers located in Asia.

These cross-border data flows are ongoing and a fundamental part of the operations of OTT platforms. They allow for real-time content delivery, worldwide analytics and scaling infrastructure. However, they are also a source of serious regulatory challenges. Such flows are known to expose personal information to varying degrees of protection, such as certain jurisdictions which offer less privacy protection as compared to others, or extensive powers of state surveillance.[9] Moreover, OTT data ecosystems can involve numerous entities, including cloud service providers and analytics companies and advertisers. This forms a multifaceted data processing chain where information can be passed through multiple jurisdictions before it gets to its final destination. This complexity makes it hard to regulate and question concerns relating to accountability and enforcement.

**Cross-Border Data Flows and the DPDP Act:**

***i. Section 16:***

Section 16[10] of the DPDP Act serves as the regulatory basis of cross-border data transfers. It takes a clearly flexible stance in comparison to the previous legislative projects in the

[8] Padma Sinha, Kajal Jain, 'TRAI's Framework for Data Centres, Interconnect Exchanges and Content Delivery Networks – An Update' (*FoxMandal Solicitors and Advocates*, 6 April 2022) < https://foxmandal.in/trais-framework-for-data-centres-interconnect-exchanges-and-content-delivery-networks-an-update/> accessed 23 March 2026.

[9] Khushi Malviya, Eeshaan Singh, 'Cross-Border Data Transfers and Data Localization Mandate Under the Data Protection Regime' (*Vidhi Centre for Legal Policy*, 18 November 2025) < https://vidhilegalpolicy.in/blog/cross-border-data-transfers-and-data-localization-mandate-under-the-data-protection-regime/> accessed 23 March 2026.

[10] The Digital Personal Data Protection Act 2023 s 16.

country. Section 16(1)[11] details that the Central Government may limit the transfer of personal data by a data fiduciary to such a country or territory outside India as may be specified. The logical implication of this is that cross-border transfers are by default, legally permissible unless prohibited. This "blacklist" or "negative list" model showcases a major deviation of the data localisation-oriented model that was envisaged previously in the Personal Data Protection Bill, 2019[12], where specific types of personal data were to be stored in India and limited in transfer to foreign countries. The DPDP Act is rather a re-evaluation of the policy, aiming at balancing the issue of data sovereignty and the economic needs of a global digital ecosystem.

Under this statute, Section 16 has no ex-ante terms on transfers, or requires data fiduciaries in the receiving jurisdiction to demonstrate the equivalent rate of protection. This is an intentional deviation of the conditional models as found in jurisdictions like European Union. Alternatively, the Indian model emphasizes the accountability of the transfer after it is complete and, therefore, incorporates the cross-border transfer into the larger compliance responsibility of the data fiduciary. This framework has significant importance for OTT platforms as these platforms are based on distributed data infrastructures, and even on global cloud service providers, such a restrictive or approval-based regime would significantly constrain its operations. The negative list model, in its turn, allows these entities to keep using global data frameworks without having to have jurisdiction-based approvals on every transfer.

There remains a certain level of legal uncertainty that comes with this flexibility afforded to these transfers. The Act lacks specifics as to on what grounds such jurisdictions can be limited, and it does not demand for reasons or any course of action prior to giving such notifications. Lack of such statutory direction brings about a system where the terms of permissible transfers depend upon executive policy, as opposed to well defined legislative standards.

### *ii. Section 16(2):*

Section 16(2)[13] states that the provisions of the DPDP Act shall not have any effect on the

[11] Ibid. s 16(1).
[12] 'Personal Data Protection Bill 2019' (PRS). https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 accessed 23 March 2026.
[13] The Digital Personal Data Protection Act 2023 s 16(2).

applicability of any other law that offers a greater degree of protection or restriction with regards to cross-border transfers. This maintains the functionality of sector-specific regulatory frameworks, which levy more restrictions on data transfers. An example of this is the circular on storage of payment data issued by the Reserve Bank of India which requires that some types of payment related information be stored with Indian jurisdiction only.[14] In the case of OTT platforms that submit subscription payment or user billing information, this presents a two-pronged regulatory burden. Although data of general users, such as viewing history or preference data, can be transferred freely in accordance with Section 16, financial data can also be subjected to the localisation requirements established by the sector regulation.

This creates a discontinuous compliance arena where various types of data on the same platform are subjected to different sets of regulations. Legally, this disintegration casts a doubt on the aspect of coherence because the DPDP Act fails to give a single framework that can be used to solve conflicts between general and sectoral obligations. Operationally, it gives an extra compliance liability on the OTT platforms, which have to separate the flow of data and make sure that various types of data are handled in such a way that they meet the relevant regulatory requirements.

Furthermore, Section 16(2) creates a type of structural irregularity within the framework where although the DPDP Act opens cross-border transfers in a general manner, at the same time, it does not exclude the existence of restrictive sectoral requirements. This duality is an indication of a larger debate within data governance in India, that is between the liberalization and control.

### *iii. Section 8:*

One of the key aspects about the DPDP Act approach towards cross-border data transfers is that it is based on accountability-based model of regulation. Section 8[15] puts on data fiduciaries a general obligation to put in place the applicable technical and organizational controls to guarantee adherence to the requirements of the Act. This requirement is independent of whether the data processing is taking place in India or being transferred to

[14] 'Storage of Payment System Data' (Reserve Bank of India) < https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995> accessed 23 March 2026.
[15] The Digital Personal Data Protection Act 2023 s 8.

a foreign country.

Unlike other points in the regimes which stipulate certain legal provisions regarding cross-border transfers, the DPDP Act lacks any reference to check of validity, generic contractual terms, and binding corporate rules. Rather, it vests data protection responsibility within the organizational structure of the data fiduciary. In practice, it implies that, in the case where the OTT platform relays personal data to a third party in a foreign country, be it any cloud service provider, analytics company or other related party, to the extent that such processing is carried out, the OTT platform is not only liable, but must also ensure that such processing has been conducted in a manner that highlights the standards imposed by the Act. This includes any and all duties associated with the data security, purpose limitation and legal process.

This section provides some flexibility that is especially beneficial to the international digital platforms. The Act does not prescriptively transfer rules and thus enables organizations to establish compliance systems which are individualized to their business models. This flexibility, however, has its own price, which is legal certainty. Without any standardized safeguards or regulatory directions, data fiduciaries will have to decide on their own what is perceived to be an appropriate measure, which may result in varying compliance practices. In the case of OTT platforms, it is both an opportunity and a threat. On the one hand, they are able to take advantage of the current global compliance systems without having to conform to strict statutory regulations. Conversely, they are responsible in full on the part of compliance and are liable to breaches that might be committed on foreign jurisdiction.

### *iv. Structured Transfer Safeguards:*

The lack of regulated protection of cross-border data transfers is one of the most influential characteristics in the DPDP framework. In contrast to the GDPR that obligates the adoption of specific legal tools, including standard contractual terms or binding corporate rules, the DPDP Act does not specify the adoption of these tools.

The absence of such tools has implications in a number of ways[16].

[16] Jidesh Kumar, 'Cross-Border Data Transfers Under the DPDP Act, 2023 and DPDP Rules, 2025: Navigating

*Firstly*, it curtails the accessibility of recognized compliance channels among data fiduciaries. Where in standardized mechanisms are in place across jurisdictions, legal certainties and an easy flow of data across jurisdictions are possible. In the Indian context, the absence of such mechanisms, implies that the compliance should be made through the general obligations and not specific instruments.

*Secondly*, the lack of safeguards is an issue that impacts the enforceability of data protection norms in other jurisdictions. Although, Section 8 places a responsibility on the data fiduciary, it does not impose direct legal responsibilities on foreign data processors which goes on to cast doubts on the effectiveness of enforcement where the data is processed in a country other than India.

*Thirdly*, it influences India's capacity to integrate with the international data protection systems. Other jurisdictions that mandate organized protection of data transfers might place more demands on transfers originating from or involving Indian entities, also causing a hindrance to the data flows and competitiveness of the Indian digital services.

**Constitutional Analysis:**

The DPDP Act must be considered against the constitutional right to privacy as was identified in *Justice K.S. Puttaswamy (Retd.) v Union of India*. The Supreme Court held that any limitation on privacy should meet the criteria of legality, legitimate purpose and proportionality. [17]

Section 16[18] of the act meets the legality criteria as it is based on the statutory authority. The legitimate aim of the section can include the need to preserve national security, support the sovereignty of data, and privacy. The proportionality, however, depends on how the government uses its power to limit data transfers. The lack of clear limitations on the scope of jurisdiction also highlights that there is an issue related to arbitrariness. Although the law is flexible, transparency and accountability can be compromised by the absence of procedural safeguards. Simultaneously, however, it should be noted that Section 16 does not directly limit

India's New "Negative List" Regime' (*King Stubb & Kasiva*, 14 November 2025) < https://ksandk.com/data-protection-and-data-privacy/indias-new-cross-border-data-transfer-framework/#five-challenges-mn-cs-must-anticipate> accessed 23 March 2026.

[17] Justice K.S. Puttaswamy (Retd) and Anr v. Union of India and Ors AIR [2017] Supreme Court 4161

[18] The Digital Personal Data Protection Act 2023 s 16.

the rights of individuals but governs the actions of the data fiduciaries. Therefore, any issues of the constitution are more probable to be concerned as pertains to specific executive functions rather than the section or the act itself.[19]

**DPDP Act and the GDPR:**

***i. GDPR in Practice:***

The European Union's GDPR[20] framework creates a systematic and rights-based policy governing cross-border data transfer. In contrast to the DPDP Act's flexible nature, the GDPR bases itself on the principle that the transfer of personal data to non-European countries should not occur without adequate safeguards being in place. This reflects the concern the EU holds to ensure that the level of data protection is guaranteed in its jurisdiction is not compromised when transferred to another country.

Under Article 45[21] of the framework, it allows for transfers to be made in cases where the European Commission has made an "adequacy decision" in relation to a third country. This decision then proves that the country has an adequate level of data protection that is essentially equivalent to the one offered in the EU. Assessing the adequacy acts as a thorough evaluation that takes into account the domestic data protection laws, the enforcement policy, and restrictions against access of information by the government.

Where there is no adequacy decision, Article 46[22] gives substitute transfer mechanisms, including most prominently Standard Contractual Clauses[23] ("**SCCs**") and Binding Corporate Rules[24] ("**BCRs**"). SCCs, a standardized contractual instrument places legally binding responsibilities on the data exporter and importer. Such clauses are enforced to

[19] Technology Law Team, 'A New Dawn: India's New Data Protection Regime Finally Takes Flight' (*Nishith Desai Associates*, 19 November 2025) < https://www.nishithdesai.com/research-and-articles/hotline/technology-law-analysis/a-new-dawn-indias-new-data-protection-regime-finally-takes-flight-15473> accessed 23 March 2026.
[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
[21] Ibid. art 45.
[22] Ibid. art 46.
[23] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016.679 of the European Parliament and of the Council.
[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) art 63.

make sure that the data protection standards remain contractually guaranteed in the event that the data is transmitted to the jurisdictions that do not enforce the same level of legal protections. BCRs on the other hand are internal compliance models adopted within multinational corporate groups to govern intra-group transfer of data into and out of various jurisdictions.[25]

The strength of this system has been reinforced by the judiciary. In *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*[26], the Court of Justice of the European Union struck down the EU-US Privacy Shield because it was not established that the laws of the destination country provided sufficient safeguards to EU data subjects, so the additional protection must be enforced. This judgment highlights the fact that the GDPR places greater importance on substantive protection as opposed to formal compliance. The regulatory aim is to make certain that the amount of protection that personal data receives follows the data regardless of the geographical location of its processing.

### *ii. GDPR and the DPDP Act and their Structural Differences:*

The DPDP Act is conceptually different to the GDPR in terms of the understanding of cross-border data governance[27]. Although the GDPR takes a conditional and a protectionist approach, the DPDP Act follows a more flexible one.

One of the major areas of divergence is the *lack of adequacy tests* under the DPDP framework. The DPDP Act does not demand for any evaluation of equivalence prior to allowing any transfers, as opposed to the GDPR. This removes a substantial regulatory barricade yet gets rid of an important method of enforcing uniform data protection norms.

Secondly, that there are *no standardized transfer safeguard*s. The GDPR offers specific mechanisms including SCCs and BCRs, which are all recognized and enforceable compliance mechanisms. Conversely, no similar instruments are specified in the DPDP

[25] Nicole Beranek, 'SCCS and COCs and BNR – Untangling the Web and Spotting the Difference' (*International Network of Privacy Law Professionals*, 26 November 2021) < https://inplp.com/latest-news/article/sccs-and-cocs-and-bcr-untangling-the-web-and-spotting-the-difference/> accessed 23 March 2026.

[26] C-311/18 *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* [2020] EU:C:2020:559.

[27] 'India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison' (*Latham & Watkins*, December 2023) < https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf> accessed 23 March 2026.

Act, which uses the general duty of data fiduciaries in Section 8 which leads to a decentralization and independent of compliance model where organizations decide on the right safeguards themselves.

Thirdly[28], an *independent regulatory oversight* is a characteristic feature of the GDPR where the supervisory authorities have the key role in ensuring compliance and approving mechanisms of transfers. In comparison, the DPDP Act gives the Central Government notable discretion especially in the issuance of limited jurisdictions which showcases a shift to an executive-led control as opposed to control by regulators.

Lastly, the GDPR strictly governs *onward transfers* by obligating that similar levels of protection be ensured at every stage of the data processing process. Looking at the example of SCCs, the recipients are subject to similar obligations as placed on the data importer during the process of transfer. No specific provision is provided in the DPDP Act that touches on these types of transfers, thus leaving room of uncertainty in instances of multi-layered or multi-jurisdictional data processing.

### *iii. Implications for Data Transfers:*

The major differences between the GDPR and the DPDP Act showcases severe implications to the extent of data protection as well as the overall design of the international data governance. The conditional nature of the GDPR means that any cross-transfers will only occur when there is sufficient protection in place, thus minimizing the risk of transferring personal data to jurisdictions that offer less effective legal protection. Conversely, the DPDP Act follows a more flexible approach in which the major focus is on the internal compliance systems of data fiduciaries. Although this improves operational flexibility, and minimizes regulatory conflict, it also opens the potential of differing standards of protection being applied across entities and jurisdictions since the efficacy of safeguards depends, in large part, on how entities interpret and enforce their obligations.

In the case of OTT platforms, this divergence means that there is a two-fold compliance problem. Though the DPDP framework allows them to work effectively in India in the

[28] 'Comprehensive Comparative Analysis of GDPR and DPDP' (*DPDP Consultants*, 18 February 2026) < https://www.dpdpconsultants.com/blog.php?id=70&title=comprehensive-comparative-analysis-of-gdpr-and-dpdp> accessed 23 March 2026.

context of the regulatory environment, their international operations must comply with more extensive regimes like the GDPR when dealing with data of the EU residents. This requires the designing of parallel compliance systems, which make it more complex and costly in terms of legal matters and operations. Lack of harmonized standards also makes compliance more difficult especially when it comes to cross-border data flows that touch on more than one jurisdiction.

Another closely related issue is the problem of interoperability[29] which can be defined as the collective functioning of cross-border data transfers between various regulatory frameworks. The DPDP Act lacks similar mechanisms at the moment. Lack of adequacy determinations and standardized transfer safeguards restricts India's opportunities to engage in structured international data transfer regimes, which may generate impediments where foreign jurisdictions may demand verifiable assurances of data protection standards.

Comparatively, the DPDP Act demonstrates a regulatory philosophy that puts the focus on flexibility and economic efficiency, whereas the GDPR is concerned with fundamental rights and systematic protection. Although both methods address the issues of the cross-border data governance, the fact that the DPDP Act is majorly based on an accountability model, without clearly formulated standards and enforcement mechanisms, casts doubt on its sufficiency in the long-term. It can also be said that the DPDP is viewed as a transitional framework whose success will rely on the formulation of subordinate laws, regulatory directions and institutional capability.[30] In such absence of development, the framework remains under-specified and not capable to support the complexities of multi-jurisdictional data flows of an increasingly interconnected digital ecosystem.

**Regulation and Enforcement Challenges:**

The DPDP framework has a number of structural constraints, which are especially apparent when working with complex and multilayered digital ecosystems such as OTT platforms. Major problems that are present are that *firstly,* there are no clear provisions that involve

[29] Varun N. Rao, Narendra Vijayasimha, 'From Legal Transfer to System Constraints: Architecting Cost-Efficient Cross-Border Personal Data Governance under India's DPDP Act' [2025] IJERT Volume 14, Issue 12 < https://www.ijert.org/from-legal-transfers-to-system-constraints-architecting-cost-efficient-cross-border-personal-data-governance-under-indias-dpdp-act> accessed 23 March 2026.

[30] Anirudh Burman, 'Understanding India's New Data Protection Law' (*Carnegie India,* 3 October 2023) < https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law> accessed 23 March 2026.

onward transfers. Although the provisions of the statute regarding the obligations of a fiduciary in Section 8 can be argued to apply to instances involving further transfer of data by a foreign processor, the provision does not explicitly specify or clarify the presence or absence of regulation over such downstream transfers. When there is no clear statutory guidance, data fiduciaries must rely on contractual terms, which is not necessarily enforceable inter-jurisdictional.

*Secondly*, there are no standardized contractual mechanisms. The DPDP Act does not specify any equivalent recognized compliance tools such as the GDPR's SCCs. Due to this, organizations are left to design contractual protection on their own which leads to varying compliance standards that create greater legal ambiguity. This leaves smaller platforms at a disadvantage as well because they might not have the means to build strong contractual frameworks.

*Lastly*, the structure is quite dependent on the executive will without strictly outlining the conditions of limiting jurisdictions. This is not that transparent, and this is worrisome in terms of predictability and could discourage investment in digital infrastructure. A rule-of-law point of view on this would be that without a codified set of standards, one may end up in a state of affairs in which cross-border flows of data are at the mercy of an evolving policy consideration, as opposed to a set of legal principles.

**Conclusion**

In conclusion, the DPDP Act provides a consistent system for cross-border data transfers by relying on a flexible, negative-list model. This is a practical policy decision which aims at striking a balance between the needs of economic development, technological advancement and regulation. The Act enables the data to circulate more freely, which suits the realities of the operation of digital platforms like OTT services that rely on internationally distributed networks.

Nevertheless, the framework is still inadequate towards providing strong data protection in the cross-border scenarios due to the lack of institutionalized protection measures, including effectiveness tests or standardized contractual solutions, which restrain the capacity of the system to ensure similar degrees of protection in each jurisdiction. In the same vein, the use of executive discretion without any clear, stated criteria raises concerns about transparency,

predictability, and possible arbitrariness.

In the case of OTT platforms, it creates a regulating environment that is both flexible and uncertain. Even though the Act allows these platforms to take advantage of international data ecosystems, it also imposes a lot of responsibility on them to ensure compliance in the absence of adequate instructions. The success of DPDP framework in the long run will, thus, be based on the formulation of subordinate rules, capacity-building of the institutions and increased correspondence to international data protection norms. Finally, a viable cross-border data governance should not just be regulated flexibly but also entrusted with normativity and enforceable protection. Lack of these factors will compromise the goal of ensuring smooth data flows with adequate protection of privacy rights of consumers.