NASSCOM®

Response to TRAI Consultation Paper on Cloud Services

December 2019

NASSCOM RESPONSE TO
TRAI CONSULTATION PAPER ON CLOUD SERVICES

We appreciate the opportunity to provide our comments in relation to this important sector, which has a wide-ranging impact on the Indian software/technology industry.

TRAI had conducted a similar initiative in 2016, through the issuance of a Consultation Paper on Cloud Computing on 10th June 2016 ("**2016 CP**"). NASSCOM, in its' responses to the 2016 CP had at that time suggested a 'light touch' approach for regulating the sector, subject to a detailed evaluation of ascertaining the need for any regulations in the first place and emphasizing upon the need for harmonization with other existing legislative and regulatory enactments applicable to the cloud services industry. TRAI's 2016 CP echoed the suggestion of a 'light touch' regulatory framework. *However, what could be an appropriate 'light touch' regulation for the Cloud Service Providers ("**CSP**") was not defined.*

1. Today, nearly four years later, we believe that the regulatory regime has evolved and is geared to provide the appropriate level of regulation. We have explained this in detail in the subsequent paras. The Indian cloud computing market is currently valued at USD 2.2 billion and is expected to grow at 30% p.a. to USD 7.1. billion by 2022.
    a. This should serve to indicate that the current regulatory framework has been beneficial.
    b. This combined with the lack of any visible market failures should provide confidence that the current regime is reasonably balanced.

2. The current CP proposed additional regulation, over and above the current regime. It indicates that the Department of Telecom ("**DoT**") would likely exercise regulatory control over CSPs indirectly through the industry bodies. For example, the CP proposes that the registered industry body and its CSP members 'may' be required to comply with the orders/directions issued by the DoT or TRAI in the future, while also being subject to requests to furnish information.
    a. The CP does not specify the nature or scope of the potential order/directions that the TRAI/ DoT may issue, thus leaving the industry apprehensive of open-ended regulations.
    b. Moreover, the CP does not provide any justification for the proposed additional regulation as it acknowledges that there are no material instances which point to a market failure.
    c. We believe that timing of any additional regulation has an important impact on the growth potential of industry and its market structure. It should not be too early, and it should not be too late. At this stage, we believe that it would be too early to contemplate additional regulation, more so, of the kind being proposed.

3. Cloud services are inherently global in nature and the government should create an enabling regulatory framework.
    a. The government should avoid unnecessary regulatory strictures. Instead, it should foster promotion of innovation and entrepreneurship.
    b. Additional regulation, of the kind being proposed in the CP, is likely to result in regulatory overlap with many other existing laws. TRAI should also note that the proposed draft Personal Data Protection Bill, 2018 ("**PDP Bill**") is likely to provide a comprehensive regulation on data and the same would apply to the CSPs.
    c. Since the 2016 CP, additional regulations have only increased the regulatory oversight on the CSPs. It appears that this has not been adequately considered in the current consultation. We have highlighted this in detail in the subsequent paras.

4. Further, the proposed regulation of CSPs, even if we set aside the view that such a regulation is not required, is likely to be unworkable.
    a. The market for industry association is based on the value that the association delivers to the industry. Any statutory based association is likely to harm the voluntary market for associations. This is more so if only one such association is promoted by the government.
    b. Moreover, industry associations adopt code of conduct on a voluntary basis. A government supervised code of conduct is likely to change the basic voluntary characteristic of associations.
    c. Further, if multiple associations are permitted to assume this role, it might result in industry association shopping by the CSPs and some associations being captured by a set of CSPs. Such a scenario is likely to undermine the objective behind any additional regulation and may lead to unintended outcomes i.e. abuse of the association platform.

5. We find that TRAI CP on CSP overlaps with the regulatory scope of Ministry of Electronics and Information Technology ("**MeitY**").
    a. The concerns are detailed in the subsequent paras.
    b. We recommend that TRAI or DOT should not plan to regulate the CSPs. If it all any additional regulation is required, it should be left to MeitY to consider and propose.

In summary, ***we recommend that the CSPs in India should not be subject to regulation by the DoT or the TRAI, directly or indirectly***. Any regulation will in turn only hurt the Indian government's flagship 'Digital India' programme[1], and the goal of creating a USD 1 trillion digital economy by 2025.[2]

---

[1] MeitY, Digital India Programme, available at https://www.digitalindia.gov.in/

[2] MeitY, India's trillion dollar digital opportunity, available at https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.

For this reason, we have not provided question-wise responses to the TRAI's queries and have instead provided an overall response to the CP.

I. Overlap with existing laws

It is necessary to acknowledge that CSPs do not operate in a legal vacuum. There are several laws which currently exist which already govern CSPs. To demonstrate that the country's cloud computing sector is sufficiently well regulated, a comprehensive outline of the existing laws and regulations that govern CSPs in India is provided below:

1. Information Technology Act, 2000 ("**IT Act**"), including the following rules under the IT Act:

    a. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**");
    b. Information Technology (Intermediaries Guidelines) Rules, 2011 ("**Intermediary Guidelines**");
    c. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**Decryption Rules**");
    d. Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("**Traffic Data Rules**");
    e. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("**Blocking Rules**");
    f. Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**CERT Rules**");
    g. Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 ("**NCIIPC Rules**");
    h. Information Technology (Electronic Service Delivery) Rules, 2011 ("**Electronic Service Delivery Rules**");

2. Consumer Protection Act, 2019 ("**CPA**").

3. CSPs will also be subject to the upcoming data protection law i.e. the draft **PDP Bill**, once it is passed by the Parliament.

We have described the applicability of these laws in detail in **Schedule I** below

In addition to the above laws set out in Schedule I, certain CSPs may also be required to get themselves registered with the regional offices of the DoT under the Terms and Conditions for Other Service Providers ("**OSP Regulations**"). The OSP Regulations mandate any provider of 'Application

Services' (which includes a wide gamut of IT Enabled Services) to register themselves with the Telecom Enforcement and Resource Monitoring ("**TERM**") Cells to be able to avail telecom resources from telecom operators.

You may note that in NASSCOM's submission to the Consultation Paper for Review of Terms and Conditions of Other Service Providers (**"OSP CP**"), we stated our position that the OSP Regulations may have outlived their relevance and utility and that the OSP Regulations should be scrapped. Notwithstanding the same, we submit that there should be no requirement for an additional registration requirement for CSPs, either through industry associations or otherwise. This only creates regulatory duplication which increases the burden for both the regulators and the CSPs and affects the ease of doing business.

II. Overlap of scope of CP with Personal Data Protection Bill, 2018

The CP prescribes mandatory provisions for the Code of Conduct for the industry body ("**CoC**")[3]. The proposed code of conduct covers various aspects of the industry body such as data security and disclosure frameworks.

It is submitted that the preparation of a 'Codes of Practice' has already been envisaged under Clause 61 of the PDP Bill. Under this provision, the Data Protection Authority ("**DPA**") will set out the Codes of Practice or will approve Codes of Practice drafted by industry associations which would set our parameters to protect the data privacy of individuals using digital services, and deal with aspects of data security, data portability, and transparency and accountability obligations as well.

Given that the Code of Practice proposed under Section 61 of the PDP Bill is substantially aligned with the CoC being proposed under the current CP, there would be a duplication of compliance and regulation. There is also substantial overlap between the regulators in terms of the scope of the activity that is sought to be regulated. In fact Clause 61 (2) of the PDP Bill clearly indicates that the DPA would undertake a comprehensive consultation process, after taking feedback from sectoral regulators prior to issuing the Codes of Practice. In these circumstances, the TRAI can voice any concerns it may have with respect to the Cloud Computing sector.

Any attempt at creating a parallel CoC mechanism for CSPs would create unnecessary confusion among the CSPs and would go against the idea of a 'light touch regulatory approach'. It will instead curb the freedom of business of the CSPs registered with the industry body and may unnecessarily constrain further innovation and competition.

III. Overlap of the Regulatory scope of the TRAI with the MeitY

[3] Annexure-I, TRAI Consultation Paper.

Under the Government of India (Allocation of Business) Rules, 1961[4], MeitY is tasked with:

i. developing policies for information technology and the internet (all matters other than licensing of the internet service provider);
ii. promoting internet, Information Technology ("**IT**") and IT enabled services

For cloud services being procured by the Government, MeitY already oversees the empanelment of CSPs as government-approved service providers under its 'MeghRaj' cloud computing initiative. To meet standards of empanelment, CSPs must evince compliance with standards on security, interoperability, data portability, service level agreements, and contractual terms and conditions[5]. Such compliance by CSPs is also thoroughly verified by way of a rigorous audit conducted by the MeitY's Standardisation Testing and Quality Certification Directorate[6]. The MeitY is also the relevant ministry in charge of administering the IT Act and it would also do so for the PDP Bill.

Considering the above, our submissions are that MeitY would be the relevant authority to evaluate the appropriateness of the regulatory regime for the CSPs.

---

4 Allocation of Business Rules, available at: https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_1187.pdf

5 Invitation for application/proposal for empanelment of cloud service offerings of CSPs, Ministry of Electronics and Information Technology, Government of India, *available at* http://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf

6 MeitY cloud computing initiative.

Schedule I – Description of Laws governing Cloud Service Providers.

I. IT Act

The IT Act sets out the requirements for, and regulates all forms of transactions which are conducted through 'electronic data interchange'. Enacted at a time of increasing digitization, the IT Act was intended to grant legal recognition to recognize electronic transactions and also to set out regulations for the use of electronic networks (including the Internet). The IT Act covers several issues that would be relevant for the purposes of the TRAI. Such requirements include, but are not limited to:

(i) Data Privacy and Security
(ii) Liability for transmission of illegal content by intermediaries (such as cloud computing operators)
(iii) Requirements to ensure safety and security to ensure protection of national security.
(iv) Punishments relating to hacking, intrusion into computer networks etc.
(v) Disclosure of cyber security incidents.

We have set out the comprehensive requirements that currently exist under the IT Act below for your reference:

S. No.	Provisions governing CSPs	Provision
1.	Contracts formed through electronic means are valid and enforceable, as provided under Section 10A of the IT Act.[7] Thus, all e-contracts that CSPs are party to, such as click-wrap agreements and terms of use, are enforceable and valid, provided they comply with the requirements of the Contract Act. As a result, any rights and liabilities agreed upon under such contracts will bind CSPs and their consumers.	Section 10A, the IT Act.
2.	Section 43A of the IT Act[8] along with the SPDI Rules requires CSPs to implement reasonable security practices and procedures. This framework comprehensively covers all data management activities of a CSP	Section 43A, the IT Act read with the SPDI Rules.

7 Section 10A, the Information Technology Act, 2000.

8 Section 43A, IT Act.

S. No.	Provisions governing CSPs	Provision
	including the collection[9], disclosure[10], retention[11], transfer[12], security[13], and use of sensitive personal information or data[14].	
3.	If CSPs fail to furnish any information, file any return or maintain their books of account or records, as per the requirements of the IT Act or the regulations made thereunder, they can be liable to pay a penalty.[15]	Section 44, the IT Act.
4.	If CSPs contravene any rules or regulations made under the IT Act, for which no penalty has been separately prescribed, they can be liable to pay up to INR 25000 for such contraventions.	Section 45, the IT Act.
5.	If CSPs access or secure access to a computer, computer system, computer network or computer resource without the permission of the owner or any other person who is in charge, of such computer, computer system, computer network or resource, they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSPs involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(a) read with Section 66, the IT Act.
6.	If CSPs download, copy or extract any data, computer data base or information from such computer, computer system, computer network or	Section 43(b) read with Section 66, the IT Act.

9 Rule 5, SPDI Rules.

10 Rule 6, SPDI Rules.

11 Rule 5, SPDI Rules.

12 Rule 7, SPDI Rules.

13 Rule 8, SPDI Rules.

14 *See* Rules 4, 5, 6, 7 and 8 of the SPDI Rules.

15 Penalty for failure to furnish any information or to file any return required to be filed within the specified time is a penalty not exceeding INR 5000 for every day such failure continues and the penalty for failure to maintain books of account or records is a penalty not exceeding INR 10000 for every day such failure continues.

S. No.	Provisions governing CSPs	Provision
	removable storage medium (*refer to point 6 above*), they can be required to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSPs involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	
7.	If CSPs person introduce any computer contaminant[16] or computer virus[17] into such computer, computer system or computer network (*refer to point 6 above*), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSPs involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(c) read with Section 66, the IT Act.
8.	If CSPs are responsible for destroying, altering, deleting, adding, modifying or rearranging any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network (*refer to point 6 above*), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(d) read with Section 66, the IT Act.

16 *Per* the explanation to Section 43, "computer contaminant" means any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network.

17 *Per* the explanation to Section 43, "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

S. No.	Provisions governing CSPs	Provision
9.	If CSPs disrupt or cause the disruption of any computer, computer system or computer network (*refer to point 6 above*), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(e) read with Section 66, the IT Act.
10.	If CSPs deny access or cause the denial of access to any person authorised to access any computer, computer system or computer network by any means (*refer to point 6 above*), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(f) read with Section 66, the IT Act.
11.	If CSPs provide any assistance to any person to facilitate access to a computer, computer system or computer network (*refer to point 6 above*) in contravention of the provisions of the IT Act or rules framed thereunder, they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(g) read with Section 66, the IT Act.
12.	If CSPs charge the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network (*refer to point 6 above*), they will have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(h) read with Section 66, the IT Act.
13.	CSPs that destroy, delete or alter any information residing in a computer	Section 43(i) read with Section 66, the IT Act.

S. No.	Provisions governing CSPs	Provision
	resource or diminish its value or utility or affect it injuriously by any means, shall have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	
14.	CSPs that steal, conceal, destroy or alter any computer source code used for a computer resource with the intention to cause damage will have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(j) read with Section 66, the IT Act.
15.	CSPs that knowingly or intentionally conceal, destroy or alter computer source codes that are required to be maintained by law can be punished with imprisonment of up to 3 years or fine of up to INR 200000 or both.	Section 65, the IT Act.
16.	Sending: (i) any information that is offensive; (ii) any false information that is likely to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will; or (iii) any message that is misleading or deceptive by means of a computer resource or a communication device is punishable with imprisonment of up to 3 years and a fine. Thus, if any CSPs are involved with the above-mentioned activities, they can be liable under this provision.	Section 66A, the IT Act.
17.	Dishonestly receiving or retaining any stolen computer resource or communication device knowing or having reason to believe the same to be a stolen computer resource or communication device is punishable with imprisonment of up to 3 years or fine of up to INR 100000 or both. Thus, if any CSPs are involved with the above-	Section 66B, the IT Act.

S. No.	Provisions governing CSPs	Provision
	mentioned activities, they can be liable under this provision.	
18.	Identity theft by way of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any person is punishable with imprisonment of up to 3 years or fine of up to INR 100000 or both. Thus, if any CSPs are involved with such identity theft, they can be liable under this provision.	Section 66C, the IT Act.
19.	Cheating by personation by means of any communication device or computer resource is punishable with imprisonment of up to 3 years or fine of up to INR 100000 or both. Thus, if any CSPs are involved with such cheating, they can be liable under this provision.	Section 66D, the IT Act.
20.	Capturing, publishing or transmitting the image of a private area of any person without their consent, and violating the privacy of such person is punishable with imprisonment of up to 3 years or fine of up to INR 200000 or both. Thus, if any CSPs are involved with the above-mentioned activities, they can be liable under this provision.	Section 66E, the IT Act.
21.	Engaging in cyber-terrorism[18] is punishable with imprisonment which	Section 66F, the IT Act.

[18] *Per* Section 66F, cyber terrorism refers to the following:

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
(iii) introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted

S. No.	Provisions governing CSPs	Provision
	may extend to imprisonment for life. Thus, if any CSPs engage in cyber-terrorism as defined under this provision, they can be liable under this provision.	
22.	Publishing or transmitting obscene material in electronic form is punishable with imprisonment and a fine.[19] Thus, if any CSPs are involved with such publication or transmission, they can be liable under this provision.	Section 67, the IT Act.
23.	Whoever publishes or transmits any material containing any sexually explicit act or conduct in the electronic form is punishable with imprisonment and a fine.[20] Thus, if any CSPs are involved with such publication or transmission, they can be liable under this provision.	Section 67A, the IT Act.
24.	Whoever publishes or transmits any material depicting children engaged in any sexually explicit act or conduct in the electronic form is punishable with imprisonment and a fine.[21] Thus, if any CSPs are involved with such publication or transmission, they can be liable under this provision.	Section 67B, the IT Act.

information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

19 Upon the first conviction, the punishment shall be imprisonment of up to 3 years and a fine of up to INR 500000 and in the event of second or subsequent conviction with imprisonment the punishment shall be imprisonment of up to 5 years and a fine of up to INR 1000000.

20 Upon the first conviction, the punishment shall be imprisonment of up to 5 years and a fine of up to INR 1000000 and in the event of second or subsequent conviction with imprisonment the punishment shall be imprisonment of up to 7 years and a fine of up to INR 1000000.

21 Upon the first conviction, the punishment shall be imprisonment of up to 5 years and a fine of up to INR 1000000 and in the event of second or subsequent conviction with imprisonment the punishment shall be imprisonment of up to 7 years and a fine of up to INR 1000000.

S. No.	Provisions governing CSPs	Provision
25.	An intermediary is required to preserve such information as may be specified for such duration and in such manner as may be prescribed by the central government. Contravention of this provision will attract imprisonment of up to 3 years as well as a fine. Thus, CSPs that do not abide by the requirements of the central government's directions specified under this provision, can be punished with imprisonment and a fine.	Section 67C, the IT Act.
26.	CSPs can be directed to co-operate with authorised government agencies to facilitate electronic surveillance[22], if it is necessary for certain reasons,[23] as per the procedure prescribed under Section 69 read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.	Section 69, the IT Act.
27.	CSPs can be directed to block public access to any information generated, transmitted, received, stored or hosted in any computer resource by the central government, if it is necessary for certain reasons. [24]	Section 69A, the IT Act.
28.	CSPs can be directed to co-operate with authorised government agencies to enable online access to traffic data for enhancing cyber security.[25] [*Refer to Table 5 for compliance requirements*	Section 69B, the IT Act.

[22] Section 69(1) of the IT Act allows authorised government agencies to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

[23] As provided under Section 69(1) of the IT Act, these reasons are: in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement of or for investigation of offence.

[24] As provided under Section 69A(1) of the IT Act, these reasons are: in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence.

[25] Section 69B, IT Act.

S. No.	Provisions governing CSPs	Provision
	for CSPs under the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009]	
29.	CSPs that fail to provide information called for by the computer emergency response team[26] ("**CERT**") or to comply with the directions of the CERT, will be punishable with imprisonment of up to 1 year or fine of up to INR 100000 or both.	Section 70B, the IT Act.
30.	Any person in possession of any material containing personal information about any person disclosing the same to another person without the consent of the person concerned or in breach of a lawful contract with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain will be punishable with imprisonment of up to 3 years or fine of up to INR 500000 or both. Thus, if any CSPs are involved with the above-mentioned activities, they can be liable under this provision.	Section 72A, the IT Act.
31.	As intermediaries under the IT Act,[27] CSPs are subject to a wide range of due diligence requirements under Section 79 of the IT Act[28] and the Intermediary Guidelines. Failure to comply with	Section 79, the IT Act read with the Intermediary Guidelines.

[26] *Per* Section 70(b)(4), the "computer emergency response team" serves as the national agency for performing the following functions in the area of cyber security: (a) collection, analysis and dissemination of information on cyber incidents; (b) forecast and alerts of cyber security incidents; (c) emergency measures for handling cyber security incidents; (d) coordination of cyber incidents response activities; (e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and (f) such other functions relating to cyber security as may be prescribed.

[27] Section 2(1)(w) of the IT Act defines an intermediary as "*any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites online auction sites, online- market places, and cyber cafes.*"

[28] Section 79, IT Act.

S. No.	Provisions governing CSPs	Provision
	these due diligence requirements will result in CSPs losing the protection of the intermediary safe harbour under this provision. The due diligence requirements for CSPs under the Intermediary Guidelines include the obligation to appoint grievance officers[29], remove objectionable or otherwise illegal content in a time-bound manner[30] and report cyber security incidents[31]. Significantly, the MeitY has recently released a set of proposed amendments to the Intermediaries Guidelines Rules ("**Draft Rules**").[32] These proposed amendments will impose additional obligations on all intermediaries, including CSPs.	
32.	CSPs are subject to the modes or methods for encryption that are prescribed by the central government under Section 84A of the IT Act and the Decryption Rules.	Section 84A, the IT Act and Rule 3 of the Decryption Rules
33.	Abetting any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by the IT Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act. Thus, if CSPs acts as abettors to any offence under the IT Act, they can be liable under this provision.	Section 84B, of the IT Act.
34.	Attempting to commit an offence punishable by the IT Act or causing	Section 84C, of the IT Act.

29 Rule 3(11), Intermediaries Guidelines Rules.

30 Rule 3(2), Intermediaries Guidelines Rules.

31 Rule 3(9), Intermediaries Guidelines Rules.

32 Comments/suggestions invited on draft of the Information Technology [Intermediary Guidelines (Amendment) Rules], 2018, Ministry of Electronics and Information Technology, *available at* http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9C-information-technology-intermediary-guidelines (Last accessed on 12 January 2019).

S. No.	Provisions governing CSPs	Provision
	such an offence to be committed, and in such an attempt doing any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both. Thus, if CSPs attempt to commit an offence under the IT Act, or cause such an offence to be committed, they can be liable under this provision.	
35.	Where any company is in contravention of any of the provisions of the IT Act or the rules framed under it, every person who, at the time, was in charge of and responsible to the company for the conduct of business as well as the company, shall be guilty of the contravention unless such person proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention. Thus, persons in charge of and responsible for cloud computing companies can be held liable for any contraventions by the cloud computing companies involved, in certain cases.	Section 85, of the IT Act.

II. CPA

The CPA protects the interests of the consumers and provides for effective mechanism for the settlement of consumer grievances. The CPA defines 'consumers' as a person who buys any good or avails a service for a consideration but does not include a person who avails of such service for any commercial purpose. Under the CPA, an order can be issued against an 'electronic service provider' to provide any information, documents or records. An 'electronic service provider' includes within it providers of '*technologies or processes to enable a product seller to engage in advertising or selling goods or services to a consumer and includes any online market place or online auction sites'*. CSPs would fall under the definition of an 'electronic service provider' under the CPA.

Additionally, buying or selling of cloud-based services would qualify as e-commerce[33] under the CPA. The central government is empowered to take measures for the purposes of preventing unfair trade practices in e-commerce. Such measures may relate to the trade practices of CSPs. The CPA also empowers a customer to file a complaint against an unfair contract[34] or unfair trade practices adopted by any service provider (which would include an e-commerce service provider).

S. No.	Provisions governing CSPs	Provision
1.	CSPs would fall under the definition of an 'electronic service provider' under the CPA.	Section 2(17) of the CPA
2.	Buying or selling of cloud-based services would qualify as e-commerce under the CPA.	Section 2(16) of the CPA
3.	The District Commission may require an electronic service provider to provide such information, documents or records.	Section 34 of the CPA
4.	The central government is empowered to take measures for the purposes of preventing unfair trade practices in e-commerce. Such measures may relate to the trade practices of CSPs	Section 94 of the CPA

III. ***PDP Bill***

The TRAI may also appreciate that the draft PDP Bill released by the MeitY already mandates 'data portability'. This essentially would mean that consumers would be able to request all of their personal data from CSPs (which act as 'data fiduciaries') and transfer their data to competing platforms. This would, effectively allow for a degree of interoperability among CSPs. As a 'data fiduciary' CSPs will be primarily responsible to comply with the obligations set out under the PDP Bill, such as Notice (that is clear, concise and

---

33 Section 2(16) of the CPA defines "e-commerce" as *buying or selling of goods or services including digital products over digital or electronic network*;

34 Section 2(46) of the CPA defines "unfair contract" means a contract between a manufacturer or trader or service provider on one hand, and a consumer on the other, having such terms which cause significant change in the rights of such consumer, including the following, namely: —

(i) requiring manifestly excessive security deposits to be given by a consumer for the performance of contractual obligations; or
(ii) imposing any penalty on the consumer, for the breach of contract thereof which is wholly disproportionate to the loss occurred due to such breach to the other party to the contract; or
(iii) refusing to accept early repayment of debts on payment of applicable penalty; or
(iv) entitling a party to the contract to terminate such contract unilaterally, without reasonable cause; or
(v) permitting or has the effect of permitting one party to assign the contract to the detriment of the other party who is a consumer, without his consent; or
(vi) imposing on the consumer any unreasonable charge, obligation or condition which puts such consumer to disadvantage;

comprehensible), purpose limitation and collection limitation, maintaining data quality, storage limitation. Further, the PDP Bill proposes that data fiduciaries should be obligated to incorporate / implement policies along the lines of a "Privacy by Design" principle, whereby privacy principles such as preventing harm, transparency, choice etc. in relation to processing and collection of personal data are built into the architecture / systems of the data fiduciary and has to implement appropriate security standards.

The PDP Bill prescribes heavy penalties which may extend to INR 15 crores/ 4% of the total worldwide turnover, and even criminal penalties may be imposed on the contravention of the obligations prescribed under the PDP Bill. CSPs will also be subject to a number of additional obligations as 'data processors' under the PDP Bill and possibly has to comply with 'codes of practice' issued by the Data Protection Authority under the PDP Bill. At the time of writing, the PDP is expected to be introduced in the 2019 Winter Session of Parliament[35].

S. No.	Provisions governing CSPs	Provision
1.	CSPs will be subject to a number of obligations as 'data processors' under the PDP Bill. These include: a. Processing data only as per instructions of data fiduciaries by whom the CSP has been engaged b. Implementing appropriate security safeguards through use of methods such as encryption and de-identification of data c. Possibly complying with 'codes of practice' issued by the Data Protection Authority under the PDP Bill	a. Clause 37, b. Clause 31 c. Clause 61 of the PDP Bill
2.	As data fiduciary CSPs will be subject to certain obligations such as: a. Purpose limitation b. Collection limitation c. Notice d. Data quality e. Data storage limitation f. Accountability g. Privacy by design	a. Clause 5 b. Clause 6 c. Clause 8 d. Clause 9 e. Clause 10 f. Clause 11 g. Clause 29
3.	Data principal has the right to data portability with respect to the personal data provided to a CSP. This would suitably address the TRAI's apprehension on data portability.	Clause 26 of the PDP Bill
4.	DPA may set out Codes of Practice to promote good practices of data protection and facilitate compliance. These Codes of Practice may be created by the DPA or	Clause 61 of the PDP Bill

35 See, https://www.business-standard.com/article/pti-stories/data-protection-bill-to-be-tabled-in-parliament-in-current-session-119111801196_1.html

S. No.	Provisions governing CSPs	Provision
	drafted by industry associations and subsequently approved by the DPA. The contents of the Codes of Practice would *inter alia* include issues of: (a) Notice requirements (b) Data Quality (c) Data Security (d) Grounds for Processing (e) Standards and Means of Data Portability (f) Data Anonymization (g) Data Retention and Deletion (h) Cross-Border Transfers And any other residual matter deemed appropriate by the DPA under the PDP Bill.	