CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY, DELHI

COMMENTS TO TRAI'S CONSULTATION PAPER ON CLOUD COMPUTING

Authored by: Kritika Bhardwaj

INTRODUCTION

Our approach to this consultation paper is based on the Centre for Communication Governance at National Law University Delhi's commitment to human rights. We have therefore limited our recommendations to those aspects of cloud computing that are likely to impact the right to privacy and have confined ourselves to a discussion of data protection and other allied concerns. This response addresses issues identified in Chapter 5 and offer answers to questions 5, 14, 15 and 17.

Broadly, we argue that a regulatory framework for cloud computing must be supported by a privacy statute and a comprehensive data-protection framework. This is supported by Ernst & Young's survey in which 72% of the respondents cited data privacy and

security as an 'extremely significant' concern in the adoption of Infrastructure as a Service (IaaS) services.[1]

We begin with a brief outline of relevant privacy law in India, to offer context for our argument that a more robust privacy framework is necessary. We then proceed to comment on questions 5, 14, 15 and 17.

Cisco's projections indicate that more than eighty-six per cent of all workloads[2] are likely to be carried out by cloud data centres by 2019.[3] If this is accurate, it is necessary to put in place a strong regulatory framework to address the risks associated with cloud computing. Of these risks, the threat to data security and privacy is widely acknowledged.[4]

BACKGROUND: OUTLINING PRIVACY LAW IN INDIA

The right to privacy, despite not being expressly incorporated in the Indian Constitution[5], has been a part of the Supreme Court's jurisprudence for over four decades. It can be traced to Justice Subba Rao's dissenting opinion in *Kharak Singh v. State of Uttar Pradesh*[6], where he held that 'liberty' under Article 21 was comprehensive enough to

[1] Ernst & Young, 'Cloud Adoption in India' (2010) <http://twelvedot.com/blog/wp-content/uploads/2011/07/Cloud_computing_adoption_in_India.pdf> accessed 5 August 2015.

[2] 'A server workload is defined as a virtual or physical set of computer resources, including storage, that are assigned to run a specific application or provide computing services for one to many users'; See infra n. 2.

[3] Cisco, 'Cisco Global Cloud Index: Forecast and Methodology 2014-2019' <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf> accessed 16 August 2016.

[4] United Nations Conference on Trade and Development, Information Economy Report 2013, 'The Cloud Economy and Developing Countries' (2013).

[5] Chinmayi Arun, 'Paper-Thin Safeguards and Mass Surveillance in India', (2014) 26 NLSI Review 105.

[6] (1964) 1 SCR 332.

include privacy.[7] In 1970, an 11-judge bench of the Supreme Court (per majority) overruled the then existing principle[8] of mutual exclusivity of fundamental rights and held that fundamental rights were interrelated.[9] This paved the way for the Court to establish a fundamental right to privacy emanating from the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech.[10]

In *Gobind v. State of Madhya Pradesh*[11], the Supreme Court had held that since the right to privacy is not absolute, it must be developed on a case by case basis.[12] Since then, the Court has upheld the right to privacy in various contexts ranging from telephone tapping[13] to narco-analysis tests.[14] The Court's jurisprudence on privacy of personal information is somewhat limited. Mostly, the issue has arisen in the context of DNA tests[15] and HIV status.[16] The Supreme Court has not yet had an opportunity to determine the contours of the right in the context of the Internet or online personal information.

In addition to the judicial rulings on privacy, data protection principles are contained within statutes. For example, Section 43A of the Information Technology Act 2000[17] ('IT Act') and the Information Technology (Reasonable Security Practices and Procedures

[7] Kharak Singh v. State of U.P (1964) 1 SCR 332 (Rao J., dissenting)
[8] A.K. Gopalan v. State of Madras 1950 SCR 88.
[9] R.C. Cooper v. Union of India 1970 SCR (3) 530.
[10] Gobind v. State of Madhya Pradesh (1975) 2 SCC 148.
[11] Gobind v. State of Madhya Pradesh (1975) 2 SCC 148.
[12] Gobind v. State of Madhya Pradesh (1975) 2 SCC 148, [28].
[13] PUCL v. Union of India (1997) 1 SCC 301.
[14] Selvi v. State of Karnataka (2010) 7 SCC 263.
[15] Bhabani Prasad Jena v. Convenor Secretary, Orissa State Commission for Women AIR 2010 SC 2851.
[16] Mr. X v. Hospital (2003) 1 SCC 500 40.
[17] Information Technology Act 2000 (IT Act 2000), s 43 A.

and Sensitive Personal Data or Information) Rules 2011[18] ('the 2011 Rules') create a data protection framework for online and electronic data in India. These rules are however inadequate[19] and fail to protect Indian users against non-Indian Cloud Service Providers (CSPs).

[18] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[19] Graham Greenleaf, 'India's Data Protection Impasse: Conflict at All Levels, Privacy Absent' (February 1, 2014) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438366> accessed 8 August 2016.

Question 5: What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Our response to this begins with a discussion of jurisdiction, to ascertain whether Indian norms extend to Cloud Service Providers. We then discuss the data protection principles that the regulator can put in places to ensure that customers have control over their data.

It is important to note the jurisdiction concerns since well crafted data protection principles will be of little use if customers cannot enforce them in or from India. We have therefore recommended that the regulatory framework should work out ways to enforce Indian law despite the inevitable difficulties that tend to surface in the context of cross-border transactions.

Before our discussion of jurisdiction and privacy norms, we would also like to note that most of the data protection principles in the 2011 Rules apply only to *sensitive* personal information.[20] 'Sensitive personal data or information' has been defined in the Rules as information pertaining to passwords, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information.[21] This is inadequate as all personal information merits protection.[22] In contrast to this, the Rules define 'personal information' as *any* information that relates to a natural person, which, either directly or indirectly, *in combination with other information available or likely to be available with a body corporate*, is capable of

[20] IT Act 2000, s 43 A.

[21] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, Rule 3.

[22] Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 'Opinion 4/2007 on the concept of personal data' (2007).

identifying such person.[23] Unlike the narrow definition of sensitive personal information, this definition acknowledges that fragments of innocuous information, when taken together may make it easy to identify a natural person.[24]

We would also like to note that the 2011 Rules do not apply to government entities, despite the fact that they collect, process and store vast amounts of personal information.[25]

Jurisdiction

The IT Act extends its jurisdiction to defendants located outside India in the event of any offence or contravention.[26] However (as discussed in detail later in this submission) this does not imply that the Indian government will actually be able to enforce its law outside India.

RECOMMENDATIONS

It will be necessary for the regulator to ensure that CSPs have offices in India or they contract with entities with offices in India such that customers affected parties are able to seek redressal for any violation of their data protection norms within India. This redressal will not automatically result from the extension of jurisdiction within the IT Act, or even from an actual court order obtained in India. It will be necessary for the Indian state to have some means of enforcement, such as seizure of assets or arrest of responsible parties, if it is to ensure compliance with Indian law.

---

[23] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 2(i).

[24] Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 'Opinion 4/2007 on the concept of personal data' (2007).

[25] IT Act 2000, s 43 A Explanation.

[26] IT Act 2000, s 1(2); IT Act 2000, s 75.

Having created a mechanism for enforcement as described above, rules framed must incorporate data protection principles. We have derived the principles in our recommendations from the data protection laws in European jurisdictions.[27] Most of these principles have been endorsed by the Report of the Group of Experts on Privacy under the chairmanship of Justice AP Shah.[28] We recommend that the following principles be incorporated in the regulatory framework for CSPs:

- ***Notice and Consent*:**
    - Customers must have sufficient notice of the CSP's information practices. These must be made available in a clear and concise manner. The CSP must offer customers the choice to opt-in and opt-out at any time. Processing must be subject to actual, informed consent from individuals. Notice must be given if there is a change in practices of the CSP.
- ***Purpose Limitation***: The data collected must be for a specific purpose(s). The CSP must ensure that personal information is processed only for the purposes specified at the time of obtaining consent.
- ***Limited Circumstances for Disclosure to the State***: Notice must include the conditions under which the CSP can be compelled to disclose personal information to a third party. Where reasonably possible, it must also include the identity of such third parties. (Also see Question 15)

[27] Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/0031, Article 6; the Directive forms the basis for data protection statutes in all European Union jurisdictions.
[28] Planning Commission, 'Report of The Group of Experts on Privacy', (2012) at p. 70.

- ***Access and Correction***: Individuals should have access to the information held about them. This must include the right to amend, correct and delete information if it is incorrect or inaccurate.

- ***Disclosure of Information:*** Disclosure of personal information must only be in accordance with conditions specified at the time of obtaining consent. A CSP must ensure that any third party that it voluntarily discloses information to will adhere to similar or higher security and privacy standards.

- ***Security:*** The CSP must have adequate safeguards in place to protect against unauthorized access, loss, processing and destruction of data.

- ***Data Breach Notification:*** In the event of breach of any of the aforementioned principles, the CSP must notify customers of such breach and inform them of the action taken as well as the remedies available to them. Where the customer is not a natural person, it must have the obligation to inform individuals whose privacy has been breached.

- ***Enforcement:*** The rules must provide for effective means of enforcement of the abovementioned principles. Specifically, in the event of breach of any of these principles, the customer as well as individuals must have accessible means for redressal of their grievances. In addition to the regulatory framework, contracts between the customer and CSP must incorporate these principles.

Question 14: The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

A recent report found that while all types of trans-border flows had raised global GDP by 10%, over 35% of this increase was attributable to cross border data flows.[29] Another study estimates that global cloud traffic is likely to quadruple between 2014 and 2019.[30] This demonstrates the ubiquity of cross-border flows in the cloud.

However, countries justify regulating cross-border flow of data for several reasons. The rationale behind such restrictions could be to prevent companies from circumventing national laws for data protection or to safeguard information against processing risks abroad.[31] Alternatively, it could also be to avoid the difficulties associated with enforcing privacy or data protection rights abroad or to enhance the confidence of consumers and individuals.[32]

However, data localisation has the potential to negate the efficiency and economic benefits associated with cloud computing as it would require customers invest in their

[29] Mckinsey Global Institute, 'Digital Globalization: The new era og global flows' (2016) <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows> last accessed 31 August 2016.

[30] Cisco, 'Cisco Global Cloud Index: Forecast and Methodology 2014-2019' (2016)http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf, accessed 16 August 2016.

[31] Christopher Kuner, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present and Future' (2011) OECD Digital Economy Paper no. 187.

[32] Ibid

own infrastructure where energy costs and security risks may be higher.[33] In a recent survey on the risks affecting data centre operations, India ranked 36 out of the 37 countries studied.[34] Such policies are also likely to have a disproportionate impact on small and medium businesses.[35]

Consequently, data localisation may not be the best solution to safeguard important or personal information against the threat from foreign surveillance or loss of privacy and can undermine such efforts.[36] The localisation of important government documents or personal information is likely to lead to aggregation of information in one electronic resource. This could make the consequence of any unauthorised access a lot more severe.[37] Further, it limits choice as customers may be forced to opt for CSPs that offer a lower level of protections compared to other CSPs offering higher levels of protection.[38] Finally, such laws have been found to be extremely difficult to enforce in practice.[39]

Under the European Union's (EU) data protection regime, restricting data-flows has been problematic despite a strong legal framework for cross-border data transfers. According to Article 25 of the European Union Data Protection Directive, personal data of individuals can only be transferred out of the European Economic Area ('EEA') if the

[33] Reema Shah, 'Law Enforcement and Data Privacy: A Forward Looking Approach' (2015) The Yale Law Journal 326.
[34] Cushman & Wakefield, 'Data Centre Risk Index' (2016).
[35] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) Vol. 64 Emory Law Journal 677.
[36] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) Vol. 64 Emory Law Journal 677, 719; Patrick S. Ryan, Sarah Falvey and Ronak Merchant, 'When the Cloud Goes Local: The Global Problem with Data Localization', (2013) Vol. 46 (12) Computer 54, 56; Daniel Castro, 'The False Promise of Data Nationalism' (*Information Technology and Innovation Foundation*, December 2013) <http://www2.itif.org/2013-false-promise-data-nationalism.pdf> accessed 5 September 2016.
[37] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) Vol. 64 Emory Law Journal 677, 717.
[38] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) Vol. 64 Emory Law Journal 677, 716.
[39] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) Vol. 64 Emory Law Journal 732.

third country in question ensures an 'adequate' level of protection.[40] In 2015, the Court of Justice of the European Union (CJEU) interpreted this standard of 'adequacy' to mean an essentially equivalent level of protection as that offered in the European Union.[41]

The problems associated with regulating cross-border transfers in the context of the Internet date back to the European Court of Justice's (ECJ) decision in *Bodil Lindqvist*.[42] In this case, the Court held that posting information on the Internet did not amount to transfer of data to a third country despite the fact that it could be accessed by anyone worldwide.[43]

Notably, the EU had also proposed the establishment of a 'One-Stop-Shop'.[44] The proposal intended to help companies conducting their business in multiple EU countries by subjecting them to only that Data Protection Authority's (DPA) jurisdiction where their main establishment was located.[45] But efforts to limit jurisdiction of other states by localising processing operations in one or few countries have been increasingly

[40] Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/0031, Article 25.
[41] Case C-362/14 Maximillian Schrems v. Data Protection Commissioner (ECJ, 6 October 2015).
[42] Criminal Proceedings Against Lindqvist [2004] QB 1014.
[43] Ibid.
[44] Note by the Presidency to the Council of Europe of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - The one-stop-shop mechanism', <http://data.consilium.europa.eu/doc/document/ST-6833-2015-INIT/en/pdf> accessed 18 August 2016.
[45] Ibid.

unsuccessful in light of recent decisions of the CJEU.[46] In the famous '*right to be forgotten*'[47] case, even the presence of a subsidiary engaged solely in advertising activities was deemed to be sufficient to establish jurisdiction.[48]

In contrast, the Cross-Border Privacy Rules System (CBPR) formulated by the Asia-Pacific Economic Cooperation (APEC) imposes compliance obligations on parties instead of restricting trans-border flow of data.[49]

India's current framework for restricting cross-border flow of data is flawed. Firstly, the restriction stems from a disparate set of laws such as the 2011 Rules and the Public Records Act, 1993. Moreover, the 2011 Rules are inadequate for a number of reasons already outlined in the answer to Question 5 above.

The previous section highlights the challenges in restricting cross-border data flows in the contemporary digital economy. To safeguard privacy in light of the difficulties associated with enforcing cross-border data transfer laws, TRAI should look at alternate methods for the incorporation of data protection norms. The General Data Protection Regulation (GDPR)[50], passed by the European Parliament earlier this year, is a good example in this regard.

---

[46] Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, (ECJ, 1 October 2015); See also Case C-131/12Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C(2014) ECR-II 317.

[47] Case C-131/12Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C(2014) ECR-II 317.

[48] Ibid.

[49] APEC Cross-Border Privacy Rules System, <http://www.apec.org/groups/committee-on-trade-and-investment/~/media/files/groups/ecsg/cbpr/cbpr-policiesrulesguidelines.ashx>accessed 18 August 2016.

[50] European Parliament and Council, Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing

Although the GDPR retains the earlier framework of requiring the European Commission to certify 'adequacy' of the level of protection offered by a third country, it nevertheless allows transfers on the basis of contractual safeguards in the absence of an adequacy decision.[51]

RECOMMENDATIONS

- A regulatory framework for cross-border data flows must balance privacy rights of individuals with the goal of ensuring that services remain efficient and cost effective.[52]

- Instead of mandating that data be stored on local servers, a better way to secure important information is to opt for de-centralised databases or encourage the use of end-to-end encryption.[53]

- Statutory rules for regulating cross-border transfers should have adequate safeguards for privacy. At the same time, they should be flexible enough to accommodate the continuous flow of data across borders that cloud computing entails.

- Any transfer of cross-border data must be pursuant to a written agreement between the customer that contracts on behalf of the individual and the CSP.

Directive 95/46/EC (2010) L 119/1 ('General Data Protection Regulation'); the Regulation will come into force in 2018.

[51] Ibid, Article 46(2).

[52] OECD, Recommendation of the Council on Principles for Internet Policy Making (2011) <http://www.oecd.org/sti/ieconomy/49258588.pdf> accessed 31 August 2016

[53] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) Vol. 64 Emory Law Journal 677. 719; Rohin Dharmakumar, 'India's Internet Privacy Woes', *Forbes India* (26 August 2013) <http://forbesindia.com/article/checkin/indias-internet-privacywoes/35971/1#ixzz2r0zriZTF> accessed 5 August 2016.

- The written agreement must incorporate the data protection principles suggested in the recommendations under Question 5.

- The agreement must set out the type of personal information collected, duration of processing, the nature and purpose of processing and the intended recipients of this personal information.[54]

- The agreements must set out enforceable standards for security and confidentiality for the CSP to maintain while transferring personal information.[55]

- The CSP must be required to inform the customer in the event a data breach occurs.[56] The individual should be able to seek redressal and compensation. For example, the original CSP may be made liable even if the breach occurs due to any act or omission by another entity entrusted with the data by the CSP.[57]

- The agreement must necessarily incorporate an enforcement mechanism that would enable an aggrieved individual to bring proceedings against the customer as well as the CSP in the event that the individual's privacy is breached. The extent of their liability for the breach must be in accordance with their responsibilities and obligations under the contract.

- There must exist a strong data protection legal regime and the option of standard contractual clauses and/or a certification mechanism by a competent statutory authority.[58]

[54] General Data Protection Regulation, Article 28(3).
[55] Ibid, Article 28(3)(b).
[56] Ibid, Article 32(2).
[57] Ibid, Article 28(4).
[58] Ibid, Article 46(2)(c) & Article 46(2)(f).

Bilateral arrangements

It may transpire in the future that cross-border data transfers are facilitated by way of bilateral data transfer agreements between India and a third country, international organisations or a specific sector within another country.[59] An example of this trend is the Privacy Shield Agreement between the EU and the US.

Under this agreement[60], the US government is under an obligation to regularly review the practices of companies receiving personal. Failure to comply with conditions can result in sanctions or removal from the list of eligible companies. Further, access by government authorities is subject to clear limitations, safeguards and oversight mechanisms. Indiscriminate bulk collection of data has been discontinued and an Ombudsperson mechanism has been established to redress grievances that arise in the context of national intelligence. The agreement also allows an aggrieved EU citizen to make a complaint to the company directly. Alternatively, they have the option of approaching their national data protection authority that would liaise with the US regulator to ensure redressal. There is also a mechanism for arbitration under the agreement. Finally, the European Commission and the US Department of Commerce have agreed to undertake a joint review to monitor compliance with the agreed principles. The report will be published annually.

[59] Ibid, Article 45.

[60] European Commission, 'Commission Implementing Decision of 12.07.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield' (2016).

From the mechanism outlined above, the following principles are instructive for India:[61]

- Strong data protection obligations on companies receiving personal data
- Effective protection of individual rights
- Clear safeguards and transparency obligations for governmental access
- Annual joint review mechanism

[61] European Commission press release, 'European Commission launches EU-U.S. Privacy Shield: stronger protection,' 12 July 2016 <http://europa.eu/rapid/press-release_IP-16-2461_en.htm> accessed 18 August 2016.

Question 15: What policies, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

The seamless flow of data across borders has fundamentally altered the notion of territoriality on which jurisdiction is based.[62] Data stored in the cloud rarely stays in a single, fixed location.[63] In fact, transfers in the cloud are swift and uncertain.[64]This makes it difficult for law enforcement agencies to gain access to information even under certain legitimate circumstances. Thus, regulatory framework for cloud computing should allow for lawful access subject to strong privacy safeguards.

LAWFUL ACCESS TO DATA STORED IN AN INDIAN CLOUD

Section 91 of the Code of Criminal Procedure allows law enforcement agencies to access stored data. The summons or written order must be issued by a Court or an officer in-charge of a police station, respectively.[65]

Alternatively, under the proviso to Rule 6 of the 2011 Rules, sensitive personal data or information can be shared with the government without obtaining consent from the provider of information.[66] This information can be shared for the purpose of verification of identity or for prevention, detection, investigation (including cyber incidents),

[62] Jenifer Daskal, 'The Unterritoriality of Data' 125 (2015) The Yale Law Journal 326.
[63] Ibid.
[64] Ibid.
[65] Code of Criminal Procedure 1973, s 91.
[66] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, Rule 6.

prosecution, and punishment of offences. The request must be made in writing and reasons for seeking such information must be recorded.[67]

Under the IT Act, Section 69 empowers the Central Government, State Government or any officers who are specially authorised to issue orders, to intercept, monitor or decrypt information generated, transmitted, received or stored in *any* computer resource. A computer resource includes a computer system, computer network, database as well as software.[68] The direction to disclose and gain access to such a resource can be directed at "any person in-charge of the computer resource".[69]

There are certain substantive and procedural safeguards built into Section 69. As such, the interception of communications under Section 69 must be carried out in the interest of:

- The sovereignty or integrity of India
- Defence of India
- Security of the State
- Friendly relations with foreign States
- Public order
- Preventing incitement to the commission of any cognizable offense relating to the above

[67] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, Rule 6(1).
[68] Information Technology Act 2000, s 2 (1) (k).
[69] Information Technology Act, 2000, s 69 (3).

Section 69B of the IT Act permits authorised entities to monitor and collect traffic data for the purpose of cyber security. Besides Sections 69 and 69B, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ('the 2009 Rules') stipulate further procedural safeguards. These safeguards are broadly based on the Supreme Court's decision in *PUCL v. Union of India.*[70]

However, these safeguards were made by way of an interim order and have been criticised. Future safeguards must be based on up to date data protection standards in order to protect Indian citizens' data.

LAWFUL ACCESS TO DATA STORED IN A FOREIGN CLOUD

The wide meaning given to the phrase 'computer resource'[71] implies that Section 69 of the IT Act is applicable even against foreign CSPs. Yet, despite the IT Act's extraterritorial application, in the absence of any physical presence or assets in India, compliance with such orders can be a challenge.

In order to overcome the difficulties associated with compliance, India should continue to negotiate Mutual Legal Assistance Treaties (MLATs) with other nations, albeit with some modifications to the mechanism. MLATs create binding legal obligations between parties to cooperate and assist one another, subject to certain conditions.[72]

---

[70] (1997) 1 SCC 301; Chinmayi Arun and Ujwala Uppaluri, 'Research Memorandum Concerning the Indian Surveillance Framework for iProbono' Centre for Communication Governance at National Law University, Delhi (2014).

[71] Information Technology Act 2000, s2(1)(k).

[72] Vivek Krishnamurthy, 'Cloudy with a Conflict of Laws' (2016), The Berkman Center for Internet & Society Research Publication No. 2016-3 <http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2733350> accessed 31 August 2016.

In the context of cloud computing however, it is possible that law-enforcement agencies (LEAs) may not know the location of the data. This could potentially create problems in requesting disclosure.[73]The existing system is also slow and riddled with bureaucratic hurdles, making it unsuitable to the pace of digital flows.[74]Thus, the MLAT system needs reforms in order to serve legitimate security interests of states. An efficient system for lawful access of information is also crucial because it makes a strong case for opposing policies that advocate data localisation or are anti-encryption.[75]

An examination of the US law in this regard is of particular interest given the number of Internet platforms headquartered there. Over the last one year, the US Department of Justice (DOJ) has been considering a proposal to allow certain certified foreign governments to access information located within the US, provided it does not pertain to a US national or an individual on US soil.[76] The essential features of the proposed legislation are as follows[77]:

- A certification process to determine whether the foreign state has a sufficient legal framework to protect privacy and civil liberties.
- Orders by the foreign government must be subject to review or oversight by a court, judge, magistrate or an independent authority.

[73] Ibid.
[74] Ibid.
[75] Jenifer Daskal, 'A new UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right' (*Just Security,* 8 February 2016) <https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/> accessed 31 August 2016.
[76] Letter from Peter J. Kadzik, Assistant Attorney General, to Joseph R. Biden, President of the United States Senate (15 July 2016) <https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf> accessed 18 August 2016.
[77] Ibid.

- Procedures and oversight mechanisms to ensure that US nationals and persons located within the US are not targeted.
- Prior notification to the Congress before certifying or entering into an agreement.
- Reciprocal rights of US law enforcement agencies to access data stored abroad.

The US is already negotiating this framework with the UK Government. If agreed to, it is possible, if not likely, that this bilateral framework may replace the existing MLAT system for lawful access to data.

IMPACT ON INDIA AND RECOMMENDATIONS

In light of the fact that major technology and cloud computing companies are based in the United States, the abovementioned mechanism becomes fairly significant. It is unlikely that India would meet the preliminary requirement of having adequate safeguards for ensuring privacy. We recommend that in order to facilitate bilateral agreements with the United States (and potentially even other states) for lawful access of data stored abroad, India should put in place robust privacy and data protection safeguards.

Any such bilateral agreement will likely be based on reciprocity, adequacy and rule of law standards. It is imperative that India amends its rule of law standards for sharing of data and adds additional safeguards to bring it in parity with safeguards offered in the United States and the European Union. This would ensure that other states do not refrain from inking a data sharing agreement with India.

Additionally, and as previously stated, the current framework that deals with these requests is the MLAT framework and India should continue to engage to reform the system to make it more efficient.

Question 17: What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

The 'un-territoriality of data'[78] makes the conventional grounds for territorial jurisdiction largely ineffective.[79] The IT Act already has extra-territorial application.[80] It also has provisions for enforcement in the event of non-compliance. Section 69 of the IT Act mandates that any person or intermediary who fails to assist the specified agency with the interception, monitoring, decryption or provision of information stored in a computer resource shall be punished with an imprisonment for a term which may extend to seven years and shall be liable for a fine. Under Section 69B, any service provider that fails to comply can be imprisoned for a period extending upto three years and is liable to pay a fine.

Further, Section 85 of the IT Act allows proceedings to be initiated against every person who is in charge of, or was responsible for the conduct of the company's business in the event of a contravention.[81] This provision also makes directors liable if the contravention took place with their consent, connivance or any neglect on their part.[82]

[78] Jenifer Daskal, 'The Unterritoriality of Data' 125 (2015) The Yale Law Journal 326.
[79] Ibid.
[80] ITA 2000, s 1 (2); ITA 2000, s 75.
[81] Information and Technology Act 2000, s 85 (1).
[82] Ibid, s 85 (2).

RECOMMENDATIONS

- We would suggest that the existing statutory framework should ideally be supplemented by collaborative measures between governments by way of MLATs or cross-border data sharing agreements.

- The proposed model for bilateral cross-border data sharing agreements potentially eliminates the role of the judiciary of the home state, to which the CSP is subject. As a result, such agreements must provide for a dispute resolution mechanism in the event that the CSP fails to comply. If the request is prima-facie legitimate and fulfills all safeguards, the home state must be required to initiate proceedings against the CSP in order to ensure compliance with the request.

- A thorough review of our procedural law for access to information by law enforcement agencies, followed by amendment of this law such that it complies with human rights and rule of law best practices is likely to be useful. The judiciaries of several democracies refuse to enforce orders that violate their domestic human rights principles - it would be strategically useful to ensure that the Indian system is sophisticated enough to comply with the global best practices in this context. This would go a long way towards ensuring that India's data requests are not easily denied.