DATA PROTECTION LAWS IN INDIA AND DATA SECURITY - IMPACT ON THE INDIA - EU FREE TRADE AGREEMENT

- *Pranav Menon*

The relations between the European Union and India have changed rapidly in recent years, from that of aid donor and recipient, to one of partnership with growth opportunities for mutual benefit.[1] In June 2007, the European Commission and the Indian government started negotiating the EU-India Free Trade Agreement[2]. One of the most ambitious negotiations, the FTA will mean a massive slashing of India's import duties and include trade in services, investment, intellectual property rights, competition policy and government procurement.[3] The FTA will have far-reaching consequences on national, state and local laws and policies that are seen to restrict free trade of European imports and therefore, on the lives and livelihoods of Indian citizens.

Among the numerous controversies surrounding the proposed India - EU FTA, the author would like to confine this piece to data protection and security issues which have arisen during the negotiations between the parties. Given the veil of secrecy that shrouds the negotiations, no authoritative text is available as regards the respective negotiating positions of the EU and India.[4] This piece seeks to provide some *insight on the India's and EU's position regarding data protection and data security measures and analyse its impact on negotiation of the India - EU Free Trade Agreement*.

Need for Data Protection in India

India is the largest source and host of data outsourcing and data processing owing to growth of the IT and BPO sector which handle and access sensitive and personal information of people around the world. There were some incidences of data theft in these sectors when certain

1. Europe Aid - India, European Commission, Available at: http://ec.europa.eu/europeaid/where/asia/country-cooperation/india/india_en.htm
2. Hereinafter referred to as FTA.
3. Executive Summary, Qualitative analysis of a potential Free Trade Agreement between the European Union and India, Centre for the Analysis of Regional Integration at Sussex & CUTS International,
4. Lee Dae-woo, India and the EU opt for partial Free Trade Agreement, Spring 2013 POSRI Chindia Quarterly.

employees sold some personal data of a large number of British nationals to an undercover reporter who worked for British tabloid 'The Sun', thereby bringing to fore India's lack of data security mechanisms.[5] Thus, owing to the vast volume and deluge of data available with these sectors in India from other jurisdictions which have stringent database protection laws, there is a growing sense of awareness and need for adequate protection of personal data in India through domestic legislation or international commitments.[6]

While data protection seems to be a fairly well known area of legislation, at least in recent times, driven mainly by the need to address privacy concerns in an information savvy world, India has not yet come up with dedicated data protection legislation. As of now, the issue of data protection is generally governed by the contractual relationship between the parties, and the parties are free to enter into contracts to determine their relationship defining the terms personal data, personal sensitive data, data which may not be transferred out of or to India and mode of handling of the same.[7] However, such contractual arrangements are not necessarily the best available remedy as in case of breach of any data security, getting an effective remedy under contractual obligations is both difficult and time consuming.[8]

Data Protection under the Information Technology Act

The Personal Data Protection Bill, based on the framework of the EU Data Privacy Directive (1996), was introduced in the Parliament in 2006 but lapsed subsequently. Prior to the Information Technology Act,[9] India did not have any legislation addressing the issue of data protection. The Preamble of the Act listed out prevention of cyber crimes and providing adequate data security measures and procedures to protect and facilitate widest possible use of Information

5. Danish Jamil & , Muhammad Numan Ali Khan, Data Protection Act in India with Compared to the European Union Countries, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 06, Available at: http://www.ijens.org/Vol_11_I_06/112206-7474-IJECS-IJENS.pdf.
6. Vidushpat Singhania, Is there a database right protection in India? Lakshmikumaran & Sridharan Attorneys, Available at: http://www.lakshmisri.com/News-and-Publications/Publications/articles/Corporate/Is-there-a-database-right-protection-in-India.
7. Vijay Pal Dalmia, Data Protection Laws in India, Vaish Advocates and Associates, 2011.
8. Arun Agarwal, Need for data protection law, The Hindu, 24th May 2005, http://www.hindu.com/op/2005/05/24/stories/2005052400481700.htm, last visited 25/12/2012.
9. Hereinafter referred to as IT Act.

Technology worldwide, as one of its main objectives.[10] However, only after several amendments subsequently did the IT Act provide for adequate legal protection for data stored in the electronic medium. It incorporated provisions regarding privacy and data protection by prescribing both civil (Section 46) and criminal (Section 72) liabilities for protecting privacy of individuals.[11]

Further Section 65, in the original IT Act provided for protection of the source code and penalized with imprisonment an fine any tampering with such computer source documents. Section 66 further provided for the definition of hacking and also the punishment for the same. The amendment to Section 66 widened the definition of hacking by including various other means to destroy or alter the data stored in a computer or access the computer in an unauthorized manner without actually mentioning the acts to be hacking.[12] Further, as per section 67C of the amended IT Act mandates 'intermediaries' to maintain and preserve certain information under their control for durations which are to be specified by law, failing which they will be subjected to punishment in the form of imprisonment upto three years and fine.[13]

The newly inserted section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.[14] In addition to the civil remedies spelled out, Section 72-A could be used to impose criminal sanctions against any person who discloses information in breach of a contract for services.[15] These amendments have widened the liability for breach of data protection and negligence in handling sensitive personal information.

Other legal developments with respect to Data Protection & Security

10. Ministry of Communications & Information Technology, Information Technology (Amendment) Act, 2008 comes into force, Press Information Bureau, October 2009, Available at: http://pib.nic.in/newsite/erelease.aspx?relid=53617
11. Naavi, Proposed Privacy Bill -2011, Privacy Seminar, Privacy India & Others, January 2011, Available at: http://cis-india.org/internet-governance/proposed-privacy-bill
12. Supra note 5.
13. Final Report, First Analysis of Data Protection Law in India, CRID – University of Namur, Available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf, p. 28.
14. R Ananthapur, "India's new Data Protection Legislation", (2011) 8:2 SCRIPTed 192, Available at: http://www.law.ed.ac.uk/ahrc/script-ed/vol8-2/ananthapur.asp
15. Rahul Matthan, IT Act and Commerce, Centre for Internet and Society, http://cis-india.org/internet-governance/blog/it-act-and-commerce

In February 2011, the Ministry of Information and Technology, published draft rules under section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold. These rules have been made in furtherance of India's recognition of a co - regulatory regime for data protection.[16] These rules are evidently an attempt at introducing the Fair Information Practice Principles and the OECD guidelines in the Indian scenario. Additionally, the Government of India, with the help of the Department of Information Technology, is currently working on a holistic law on data protection based on the European Union directive.[17]

The recent Justice AP Shah Report on Privacy provides for multidimensional and inclusive understanding of the right to privacy to include concerns surrounding data protection on the internet and challenges emerging therefrom.[18] The privacy approach paper also suggested masquerading a data protection regime through a privacy legislation to address regulations on collection, control, utilization and proper disposal of data, which are not covered under the purview of the existing IT Act.[19] It recommends the applicability of such a regime to public as well private entities and proposes a distinction between personal data and personal sensitive data. CIS, in their response to the paper, urged that the benefits to international trade should be taken into consideration when determining the stringency of a data protection regime, and this should inform the terms of the statutes that are enacted.[20]

With respect to data security, this paper recommends that the proposed legislation must prescribe technology neutral measures to be taken by the data controllers to ensure the security of data under its control from unauthorized access, deletion, disclosure and alteration. It also suggests

16. Data Security Council of India, Strengthening Privacy Protection through Co-Regulation, NASSCOM Initiative.
17. Data Protection in India, Mazumdar & Co, Available at: http://www.majmudarindia.com/pdf/Data%20Protection%20in%20India.pdf
18. Justice AP Shah, Report of the Group of Experts on Privacy, Planning Commission, Govt. of India, October 2012, Available at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf
19. Rahul Matthan, Approach Paper for a Legislation on Privacy, Draft for Discussion, October 2010, Available at: http://ccis.nic.in/WriteReadData/CircularPortal/D2/D02rti/aproach_paper.pdf
20. Elonnai Hickok, C.I.S Responds to Privacy Approach Paper, The Centre for Internet and Society, November 2010, Available at: http://cis-india.org/internet-governance/blog/privacy/c.i.s-responds-to-privacy-approach-paper

supervision by a data regulator to seek effective implementation of these measures and ensuring credibility and integrity of the data controllers handling the information.[21]

European Union's Privacy and Data Protection Standards

The European Union lays down a very high threshold for understanding the concept of privacy. According to them, privacy can be understood as the right of an individual to be free from unauthorized intrusion and the ability of that individual to control and disseminate information that identifies or characterizes the individual.[22] This understanding of privacy is reflected in the data protection laws across countries in the EU and the EU Data Protection Directive.

The European Union Data Protection Directive has been called "the high-water mark of substantive legal protection for information privacy" and, due to its transborder transfer restrictions, "the closest approximation to a strong global data protection standard in operation."[23] The existing EU Directive encourages co-regulation and is considered a model on which the national data protection laws of several European countries have been framed.[24] The EU recently in January 2012 came up with another draft General Data Protection Regulation,[25] which modified existing principles and introduced new ones such as data minimization principle, transparency principle, clarifications on conditions of consent of the data subject to facilitate data processing, accountability of data controllers, carrying out data protection impact assessments, drafting codes of conduct covering various data protection sectors, right to data portability, mandatory data breach notification requirements, employing data protection officers for public authorities and large companies, etc.[26]

21. Ibid.
22. Supra note CIS.
23. J. Keele, Privacy by Deletion: The Need for a Global Data Deletion Principle, Indiana Journal of Global Legal Studies, Vol. 16, No. 1 (Winter 2009), pp. 363-384, http://www.jstor.org/stable/10.2979/GLS.2009.16.1.363, p. 372.
24. Supra note 15.
25. Draft 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), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
26. Supra note 17.

Article 25 of the EU Data Protection Directive,[27] contains a requirement for data to be transferred outside of the EU in order to fulfill their high privacy standards. It mandates member states to provide for transfer of personal data to third countries only where the states are satisfied that the third country in question ensures adequate level of protection, which is to be determined taking into account all circumstances relevant to the transfer particularly, the nature of data, purpose and duration of the transfer, the country to which data is being transferred and its laws and regulation.

Thus, as per this provision, data related to European citizens can be transferred outside EU borders only if the legal system of the host country provides a similar degree of protection.[28] The EU requires other countries to create independent government data protection agencies, register databases with those agencies, and in some instances, the EC must grant prior approval before personal data processing may begin.[29] This law mandates that European countries doing outsourcing business with countries that are not certified as data secure have to follow stringent contractual obligations which increases operating costs and affects competitiveness.[30]

From the perspective of EU investors, the main issues with respect to India include the relatively weaker IPR enforcement in India, problems of counterfeiting and piracy as compared to the EU, which has a negative effect on the ease of doing business in India for EU investors in sectors that are highly reliant on IP protection.[31] According to them, the lack of an efficient data protection mechanism makes confidential information pertaining to certain sectors vulnerable to copying and misuse. European industry representatives are worried about India's expansion of its share of the European outsourcing market, which already stands at 30 percent of India's $100 billion IT

27. Council Directive 95/46, Article 25(1), October 1995 O.J. (L 281) 3124 , Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML,.
28. Osvaldo Saldias, Cloud-friendly regulation: The EU's strategy towards emerging economies, Internet Policy Review, April 2013, Available at: http://policyreview.info/articles/analysis/cloud-friendly-regulation-eu%E2%80%99s-strategy-towards-emerging-economies
29. Susan Aaronson, Internet Governance or Internet Control? How To Safeguard Internet Freedom, Cicero Foundation Great Debate Paper, No. 13/01, February 2013, Available on: http://www.cicerofoundation.org/lectures/Aaronson_Internet_Governance.pdf
30. PTI, India- EU FTA Talks Fail to Bridge Gaps, Available at: http://www.livemint.com/Politics/jO5DSVLjGMUay9mopfMPGL/IndiaEU-FTA-talks-fail-to-bridge-gaps-ministerial-meet-unl.html
31. Final Report, Trade Sustainability Impact Assessment for the FTA between the EU and the Republic of India, TRADE07/C1/C01 – Lot 1, ECORYS, Cuts International & CENTAD, May 2009, Available at: http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143372.pdf.

and business process outsourcing industry, possibly resulting in the compromise of some personal data.[32]

India's want for Data Secure Status

Owing to the importance of cross-border data flows to or from the 27 countries of the EU, developing nations such as India and China are finding it difficult to make their laws interoperable with the EU's stringent privacy provisions, thereby affecting the trade policies.[33] The Data Security Council of India estimates that outsourcing business can further grow by $50 billion per annum once India is recognized as a "data secure" destination.[34] India has demanded for granting of a data secure status by the EU and incorporating an investment protection clause in the FTA in the recent talks. The EU's refusal to grant such a status to India has prevented the flow of data, including such information which may vital for India's IT services industry wanting an outsourced market access.[35] It also obstructs the free flow of sensitive information to India, such as information about patients for telemedicine, under data protection laws in the EU. [36]

This has also impacted the movement of people through restrictions on business development as it restricts transfer of personal data to locations outside EU, unless the importing country ensures adequate data protection. This increases operating costs for India companies, affects competitiveness and decreases confidence of European firms in doing business in India. India has been arguing that since US has a safe harbour pact with the EU, and that the US and India have a data adequacy agreement; therefore the EU should give data adequacy status to India.[37]

Proposed Compromise

32. Asia Briefing, India-EU Free Trade "Early Harvest" Deal Looks Possible, May 2013, Atlantic Sentinel, http://atlanticsentinel.com/2013/05/india-eu-free-trade-early-harvest-deal-looks-possible/
33. Interview with Rosa Barcelo, Privacy Coordinator, Policy Coordinator , European Commission DG CONNECT, 7/24/2012. Also see Gregory Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Data Privacy Standards," Yale Journal of International Law 25, Winter 2000, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=531682.
34. Dr. Dinoj Kumar Upadhyay, India-EU FTA: Building New Synergies, Indian Council for World Affairs, November 2012, http://www.icwa.in/pdfs/VPIndiaEUTFA.pdf.
35. PTI, EU talks on FTA expected to make headway, Hindustan Times, April 2013, http://www.hindustantimes.com/world-news/Europe/India-EU-talks-on-FTA-expected-to-make-headway/Article1-1044596.aspx
36. Deepak Rao, What to expect from the India-EU FTA, http://www.gatewayhouse.in/what-to-expect-from-the-india-eu-fta/
37. PTI, Small gap posing difficulty in finalising India-EU FTA : Rao, Financial Chronicle, June 2013, Available at: http://www.mydigitalfc.com/news/small-gap-posing-difficulty-finalising-india-eu-fta-rao-210

The European Commission has been stressing that the issue of data protection adequacy should remain separate from the FTA and that India must meet the EU requirements for adequacy under the process set out in the 1995 Data Protection Directive. The Indian government argues that the existing laws meet the required EU standards and is compliant with the European law on data protection.[38] With the EU currently revising its data protection rules, this remains a front page issue and the Commission will not want to lose face by seeming to grant data adequacy as a concession to sign an agreement.

NASSCOM on discussion with the EU Chief Negotiator regarding this issue got some positive indications, with the EU expressing a clear willingness to work alongside India to plug the gaps and secure adequacy status.[39] The EU has expressed willingness to set up a Joint Working Group (JWG) to look into these issues. It is hopeful that the proposed privacy legislation in India will resolve the issue of data protection and further India's bid for a data secure destination as per the EU Directive. Such a development will also determine the future of the proposed India - EU FTA.

38. PTI, India to EU: Declare us a data secure country, Times of India, October 2012, Available at: http://articles.timesofindia.indiatimes.com/2012-10-18/software-services/34554412_1_india-under-data-protection-flow-of-sensitive-data-india-and-eu.
39. EU-India FTA Discussions Gather Steam, NASSCOM, Available at: http://www.nasscom.in/euindia-fta-discussions-gather-steam?fg=235321