ORF ISSUE BRIEF
DECEMBER 2019
ISSUE NO. 332

An Assessment of the Bulk Data Sharing Policy of the Ministry of Road Transport and Highways

SHASHIDHAR K.J.

ABSTRACT In March 2019, the Ministry of Road Transport and Highways (MoRTH) rolled out the Bulk Data Sharing Policy for its databases. The policy states that organisations must pay an annual fee of INR 3 crore, and research and education institutions INR 5 lakh, to access the databases in four data dumps.[1] In the absence of a data protection law, sectoral regulators and ministries are issuing their own data policies. Though the policy claims that the data being shared will be anonymised,[2] the data parameters that have been published can easily be used to identify a user and thus pose significant privacy risks. This brief examines the gaps in the MoRTH's current Bulk Data Sharing Policy. It highlights the need to protect citizens' right to privacy and makes recommendations to improve the policy.

Attribution: Shashidhar K.J., "An Assessment of the Bulk Data Sharing Policy of the Ministry of Road Transport and Highways", *ORF Issue Brief No. 332*, December 2019, Observer Research Foundation.

ISBN 978-93-89622-26-3

INTRODUCTION

Data is at the heart of the Fourth Industrial Revolution (4IR). Rapid strides in Information and Communication Technologies (ICT) have allowed the generation, storage and processing of unprecedented amounts of personal data. It is estimated that by 2020, 50 billion devices will be wirelessly connected to the internet.[3] As data becomes increasingly important, data policies around the world must deal with the crucial issues of privacy, data protection and security in the digital world. In the digital context, data protection includes the right to have information about oneself processed fairly, i.e. ensuring that entities collect accurate information. Additionally, users must have the right to not have their data collected.

India's view on data is evolving and appropriate policies on data need to be implemented. Currently, India does not have explicit legislation regulating the flow of data. A Personal Data Protection Bill has been introduced in Parliament. The Information and Technology (IT) Act deals with some aspects of data protection.[4] Under the Act, some protection is given to "sensitive personal data," as defined below:

"Sensitive personal data or information of a person means such personal information which consists of information relating to:

(i) password;

(ii) financial information such as bank account or credit card or debit card or other payment instrument details;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise"

This definition, however, applies only to corporations processing data about individuals, and not to government data. India's official policy for sharing non-sensitive data collected by the government on a bulk basis, i.e. where users can download all of the information stored in a database at once, is called the National Data Sharing and Accessibility Policy (NDSA). The NDSA enabled the creation of an Open Government Data (OGD) platform.[5] As part of the OGD, the government created a website called *data.gov.in*, where it would provide collated access to datasets, apps and catalogues published by different government entities and ministries at periodic intervals. The OGD platform has been publishing data sets since 2012. It now collects data from 162 departments and has 19,819 application programming interfaces (APIs). However, the NDSA does not specify how government data can be monetised.

In 2011, the Ministry of Road Transport and Highways (MoRTH) created the *Vahan* and *Sarathi* databases under its National e-Governance Policy, through which it would release funds to state Regional Transport Offices (RTOs) to digitise legacy data.[6] The Vahan database digitises all vehicle

registration records, while the Sarathi database digitises driver's licence information. The data is considered non-sensitive personal data. MoRTH appointed the National Informatics Centre (NIC) to set up the databases. Initially, the project was allotted INR 148 crore.[7] To digitise their legacy records, states and Union Territories were paid INR 5 per document. States such as Arunachal Pradesh and Jammu and Kashmir, which have more difficult terrain, were paid INR 7.[8]

In July 2019, answering a question posed in the Upper House of Parliament, India's Union Minister for Road Transport and Highways Nitin Gadkari revealed that the government had earned INR 65 crore as of July 2019, by selling access to the Vahan and Sarathi databases to about 87 private and 32 government entities. The databases include information on 25 crore vehicle registrations and 15 crore drivers' licences.[9] However, a right to information (RTI) query showed that the MoRTH had actually shared access with 142 companies, including 30 public and private sector banks, 20 logistics solution providers, 19 finance organisations, 18 insurance organisations and five automobile manufacturers.[10]

In March 2019, the MoRTH put in place a formal Bulk Data Sharing Policy. Under this policy, commercial organisations will have to pay INR 3 crore to obtain access to the Vahan and Sarathi databases for one year. The data will be provided in four dumps in an encrypted format. Education institutions and researchers can access this data for INR 5 lakh. From fiscal year (FY) 2020–21, there shall be an annual increment of five percent.[11] According to MoRTH officials, information to third parties will be disclosed in an anonymised form, i.e. with all personally identifiable information removed.[12] As per the Bulk Data Sharing Policy, companies will have access to 28 parameters of the Vahan database, which include the following:

1. Registration Number
2. Engine Number
3. Chassis Number
4. Class of Vehicle
5. Purchase Date
6. Registration Date
7. Registering Authority
8. Manufacturer Name
9. Model Name
10. Body Type
11. Fuel Type
12. Wheelbase
13. Number of Cylinders
14. Colour
15. Dealer
16. Seating Capacity
17. Standing Capacity
18. Gross Vehicular Weight/ Laden Weight
19. Unladen Weight
20. Cubic Capacity
21. Horsepower
22. Financer's Name (Hypothecation)
23. Insurance Company Name
24. Insurance Validity
25. Fitness Validity
26. Permit Type

27. Permit Validity
28. Tax Paid Validity

Further, the MoRTH has released an application called *mPariVahan*, which allows users to obtain basic details about a particular driver's licence and registration certificate, i.e. owner's name and recent traffic violations. "The purpose of this information is to promote statutory compliances and also facilitate individual hiring/ renting or purchase/sale of vehicles and hiring of drivers," the policy reads.[13]

WHY IS THE GOVERNMENT SELLING THIS DATA?

The MoRTH's policy addresses a genuine need for certain companies and security authorities to be allowed access to driver's licence and vehicle registration data. For example, such data will be significant in helping customers ensure that the second-hand vehicle they are buying is a legitimate commodity and not being fenced. Additionally, insurance companies can use the data to expedite claims processes in cases of accidents.

India's policy papers often start with the phrase "data is the new oil,"[14] and many Indian policymakers view citizen data as a natural resource. In June 2019, the Osaka Track of the G20 pushed hard for the creation of laws that would allow easier data flows between countries and prevent data localisation. Consequently, India boycotted[15] the Osaka Track of the summit. Indian Foreign Secretary Vijay Gokhale called data a new form of wealth and insisted that India needed greater latitude to frame its policies regarding its citizens' data.[16] According to a McKinsey report, the size of India's digital economy in 2017–18 was approximately US$200 billion, and the government has an ambitious plan for expanding it into US$1 trillion by 2025.[17]

In this context, policymakers are pushing for data localisation to ensure that its citizens' data resides in the country. Further, they are advocating for Indian companies to have access to this data so that they can monetise it. This is underscored in the Economic Survey 2018–19 by the Ministry of Finance, which dedicated a chapter to how the Indian government could monetise citizen's data.[18] The survey states that data should be treated as a public good and calls for the creation of a central welfare database of citizens, with each ministry acting as a data fiduciary (any entity or person that processes personal data). The document further recommends that private companies be allowed to access the database for a fee, considering the potential to reap massive dividends from citizen's data.

However, the notion that "data is the new oil" is problematic, to begin with: it views data from the prism of profitability—to be harvested, stored and traded. This reduces people's data to a commodity that can be bought or sold without their consent. While talking about treating "data as public good," the Economic Survey of India argues that the "elite's preference for privacy should not be imposed on the poor, who care for a better living the most." However, the idea that governments and private companies do not need consent from citizens to process their personal data directly contradicts the 2017 landmark Supreme Court judgement that upheld privacy as a fundamental right.

The Indian Parliament is still debating the Personal Data Protection Bill. In the interim, India does not have any legal safeguards to protect user data. By claiming ownership of citizens' data and selling access to them, the government has eroded privacy concerns and created significant privacy risks.

RISKS OF PRIVACY BREACH

The MoRTH's Bulk Data Sharing Policy acknowledges the possibility of *triangulation*, i.e. the matching of different datasets that together could enable individuals to be identified and their privacy compromised.[19] According to the policy, it is solely the company's responsibility to ensure that a person is not identified through triangulation. Further, during security audits, if the ministry finds that the protocol of data use that has been followed is not in line with the one prescribed, the company or person will be liable for any action permissible under the IT Act and will be banned from access to this data for a period of three years.[20]

However, there are no controls to *actually* prevent a company or individual from linking the Vahan and Sarathi database with other data sets. For example, a company can make a new database using the mPariVahan app, obtain owner details of cars and link them with existing Know Your Customer (KYC) details. Thereafter, the company will be able to profile the owner's entire vehicle usage history.

MoRTH officials insist that the data will be provided in an anonymised format. However, the policy specifically states that the ministry shares the complete data with certain enforcement agencies, banks, automobile industries, finance companies and insurance companies. This effectively nullifies any efforts of anonymisation, since banks, finance companies and insurance companies—essentially third parties—are being allowed access to personally identifiable information. While it is possible that the MoRTH is giving access to these databases as part of the NDSA, it is not sufficient to protect the privacy of individuals. According to the NDSA, every department or ministry must create a negative list, i.e. datasets that are confidential in nature and can compromise the county's security if made public, which only includes personal information. Therefore, the only piece of data that is not given out based on the MoRTH's policy is the address of a vehicle owner and that of the driver's licence holder.

The loss of privacy due to the compromise of name, vehicle information and traffic violations (combined with other datasets) can have devastating impacts on citizens. The Electronic Frontier Foundation (EFF) chronicled abuses by law enforcement officials of the California Law Enforcement Telecommunications System (CLETS), a computer network that grants the police access to criminal histories and driver's records.[21] The EFF's investigations brought to light 143 instances in 2017, in which the CLETS system was abused; this included police officers accessing confidential information for domestic disputes, running background checks for dates, and handing over witness information to the family of a convicted murderer.[22] The CLETS network is accessed 2.8 million times a day, and there could be a larger number of instances of abuse that have gone unreported.

If information from the mPariVahan application is combined with KYC data, it is not difficult to imagine a situation in which a person is stalked or put under illegal surveillance. On a broader systemic level, traffic violation data may be used to discriminate against citizens. Additionally, since the design of machine-learning algorithms is underlined by data, it becomes imperative that such data is absent of bias or anomalies, which may become a source of discrimination. For example, as algorithms play an increased role in deciding loans using multiple data points, higher interest rates or insurance premiums might be levied on certain individuals or communities. Using artificial intelligence to make decisions about users and customers can be dangerous when the algorithms inherit biases from older datasets, which might affect a whole community.

In the US, African-Americans and other people of colour receive more traffic citations or violations as compared to Caucasian drivers.[23] Researchers Betsy Anne Williams, Catherine F. Brooks and Yotam Shargad point out that even if a person or entity decides to withhold or delete information, algorithms using Big Data will be able to sufficiently identify a person or a group using proxies that reflect the omitted information.[24]

In his book, *Unravelling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future*, Scott R. Peppet asks, "How long before one's unwillingness to put a monitor in one's car amounts to an admission of bad driving habits, and one's unwillingness to wear a medical monitor leads to insurance penalties for assumed risky behaviour?"

WHO OWNS THE DATA?

With the government selling access to the Vahan and Sarathi databases, it is worth debating who owns the vehicle registration and driver's licence data, considering it is information about an individual. Does the government own the data or does the individual? What rights does a citizen have over data pertaining to them? Can the government sell this data?

The *K.S. Puttaswamy vs. Union of India and Ors* Supreme Court judgement upholds that privacy is a *fundamental* right, although not an *absolute* right. It mentions that the state is obligated to protect an individual's private data subject to certain reasonable restrictions.[25] However, it explicitly roots a person's privacy interests in dignity and autonomy, not in any notion of property. Since the digitisation of vehicle registration and records were carried out using funds from the ministry as part of its e-governance policy, the government is claiming ownership of the data arguing against the assertion that the data belongs to the individual. The proposed Personal Data Protection Bill defines data as follows:

> "Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information."[26]

Under this definition, vehicle registration and driver's licence data can be considered personal data. The proposed Personal Data

Protection Bill preserves certain rights of a data principal—defined as the natural person to whom the personal data relates to—and requires companies to take consent from and give notice to the data principal before processing personal data.[27]

This definition, however, contradicts the government's claim of ownership of the data pertaining to its citizens. Thus, when the MoRTH sells access to the Vahan and Sarathi databases, it is selectively applying the Property Rights Framework. A key point of the Property Rights Framework is the exclusivity of ownership. For example, a car cannot be sold to multiple people. However, access to data is being sold to multiple entities. What are the long-term implications of data being bought, sold, leased and treated as property? What happens when the value of a dataset appreciates? Would long-term capital gains tax be applicable to data? The government needs to develop a more nuanced understanding of what data is before assigning to it different rights frameworks.

RECOMMENDATIONS FOR MORTH'S BULK DATA SHARING POLICY

The MoRTH's current Bulk Data Sharing Policy must be revamped to protect the privacy of Indian citizens.

1. The scope of what is considered personal data must be broadened. The IT Act only offers protection to "sensitive personal data," which is defined very narrowly. The older definition of the IT Act might have sufficed for the IT sector in the 1990s. However, the Act has not kept pace with the exponential progress in ICT.
2. The Personal Data Protection Bill must be passed after sufficient consultations with various stakeholders.
3. The MoRTH should recognise the definition of "personal data" as stated in the proposed bill and apply the protections guaranteed under it to users, to prevent misuse. The ministry must revisit the section of the policy that allows third parties access to driver information. The language used in the policy is vague and must explicitly specify the agencies and type of companies that will be allowed to access this data.
4. Agencies and companies, in their contracts, must specify how they will use the data, so that they can be held accountable. Additionally, these companies cannot be allowed to hold on to the MoRTH's data indefinitely. A security audit must be performed after the expiry of the time period for holding the data. This will prevent any breach of contract, such as in the case of Facebook, wherein the company does not know whether the personal data obtained from it was deleted by Cambridge Analytica as per their agreement.[28]
5. Finally, citizens should be allowed to know which company or entity has access to their driver's licence and vehicle registration data. They must also have the option to revoke access to their data.

CONCLUSION

Data cannot be treated as a commodity to be exploited by a few technology companies, whether Indian or foreign. While it is cheap to

gain access to data in the current landscape, ultimately, algorithms, software and intellectual property are what hold true value.

The Government of India puts great emphasis on data protectionism and treating data as a form of wealth. However, the MoRTH's Bulk Data Sharing Policy belies this. A back of the hand calculation suggests that if a database of 25 crore vehicle registrations is being sold for INR 3 crore, the details of each individual car is worth only INR 8.3. To put this in perspective, the Interactive Advertising Bureau (IAB) estimates that in 2017, US-based firms spent US$10.14 billion to get third-party audience data and US$563 million on data related to identity.[29]

As surveillance capitalism increases, there is now a growing movement that advocates for individuals to own their data and be compensated for the same. As Silicon Valley investor Roger McNamee asks, "Is it legal for companies to share and sell data without customers' knowledge or consent?" Amazon, for instance, claims that it is paying US$10 to its Prime users so that it can track websites that users visit, to get data that would strengthen its retail business.[30] In India, Google Pay's cashback offers can be viewed as compensation for users in exchange for financial data.[31] "There is no way companies should be allowed to collect user data and claim ownership to it. We cannot retrieve our data, but we should be able to able to control how it is used. Each person should own his or her data and be free to move it or sell it in a competitive marketplace," McNamee says.

Technology companies claim that collecting vast amounts of data will help them develop more products for future use. However, as more invasive methods of data collection are deployed, scholar Shoshana Zuboff warns, the value accrued to the user by the new products developed will be less than that accrued to the company. Yet, the users modify their behaviour assuming that they make gains.[32] She cites Google as an example and explains how it gains data surreptitiously and inflates the value of online advertising.

"Google understood that if it were to capture more of these data, store them, and analyze them, they could substantially affect the value of advertising. As Google's capabilities in this arena developed and attracted historic levels of profit, it produced successively ambitious practices that expand the data lens from past virtual behavior to current and future actual behavior. New monetization opportunities are thus associated with a new global architecture of data capture and analysis that produces rewards and punishments aimed at modifying and commodifying behavior for profit," she says.

Companies and governments undervalue data about persons, since there are no proper privacy regulations for the digital world. Concerns for privacy automatically translates into a higher valuation of data. With the government's animus for monetising data, the government is ignoring the privacy risks associated with exposing the personal data of citizens at large. Respecting privacy requires acquiring consent from individuals before using their data. The judgement that upheld the right to privacy was based on Articles 14, 19 and 21 of the Indian Constitution, which guarantee the right to life and personal liberty,

freedom of speech and expression, and equality before the law. The MoRTH's privacy-eroding policies could contribute to behaviour modification, curtailing people's personal liberty. Since citizens do not have a say on how or where their data can be used, the MoRTH's policy also infringes on an individual's right to expression. Thus, the government claiming ownership over driver's licence and vehicle registration data and selling it to different parties violates fundamental principles of freedom and liberty. In light of this, the Bulk Data Sharing Policy must be reworked as a matter of priority. ORF

ABOUT THE AUTHOR

Shashidhar K.J. is an Associate Fellow at ORF, Mumbai.

ENDNOTES

1. Question 1698, Answered on 8 July 2019, by Union Minister Nitin J. Gadkari, Rajya Sabha Website, https://rajyasabha.nic.in/.

2. *Bulk Data-Sharing Policy and Procedure*, Ministry of Road Transport and Highways, March 2019, accessed 31 August 2019, https://parivahan.gov.in/parivahan/sites/default/files/NOTIFICATION%26ADVISORY/8March%202019.pdf.

3. Mark Hung, ed., *Leading the IoT: Gartner insights on how to lead in a connected world* (Gartner Publications, 2017), accessed 28 October 2019, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

4. Notification from Ministry of Communication and Information Technology, *The Gazette of India: Extraordinary*, Department of Information Technology, 11 April 2011, accessed 31 August 2019, https://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.

5. Notification from Ministry of Science and Technology, *The Gazette of India*, Department of Science and Technology, 12 March 2012, accessed 38 October 2019, https://data.gov.in/sites/default/files/NDSAP.pdf.

6. Srinivas Kodali: Right to Information, Documents shared with author, 18 July 2019.

7. Anita Mittal and Dr. Mahesh Chandra, *Case Studies on e-Governance in India: Road Transport MMP – Vahan and Sarathi*, National e-Governance Plan, accessed 31 August 2019, http://nisg.org/files/documents/UP1418304047.pdf.

8. Ibid.

9. Question 1698, op. cit.

10. Soumyarendra Barik, "SBI, Mercedes and ICICI Lombard among the 142 entities that bought vehicle registration data from government," *Medianama,* 10 September 2019, accessed 28 October 2019, https://www.medianama.com/2019/09/223-142-entities-that-bought-vahan-data/.

11. *Bulk Data-Sharing Policy and Procedure*, op. cit.

12. Anisha Dutta, "Government clears policy to sell vehicle registration data," *The Hindustan Times*, 13 March 2019, accessed on 29 August 2019, https://www.hindustantimes.com/delhi-news/govt-clears-policy-to-sell-vehicle-registration-data/story-n4aBtGpJgETNuN9vbAW3LL.html.

13. *Bulk Data Sharing Policy and Procedure*, op. cit.

14. Ministry of Commerce and Industry, Draft National e-Commerce Policy, Department for Promotion of Industry and Trade, 23 February 2019, accessed 29 August 2019, 8, https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

15. D. Ravi Kanth, "India boycotts 'Osaka Track' at G20 summit," *Livemint*, 30 June 2019, accessed

31 August 2019, https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html.

16. Suhasini Haidar, "At G20, India stands with developing world—not U.S., Japan—on 5G and data," *The Hindu*, 28 June 2019, https://www.thehindu.com/news/national/on-5g-and-data-india-stands-with-developing-world-not-us-japan-at-g20/article28207169.ece.

17. Noshir Kaka, Anu Magdavakar, Alok Kshirsagar, Rajat Gupta, James Manyika, Kushe Gupta and Shishir Gupta, *Digital India: Technology to Transform a Connected Nation* (McKinsey Global Institute, March 2019), accessed 29 August 2019, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/digital-india-technology-to-transform-a-connected-nation-full-report.ashx.

18. Chapter 4, *Economic Survey 208–19*, Ministry of Finance, Government of India, accessed 29 September 2019, https://www.indiabudget.gov.in/conomicsurvey/doc/vol1chapter/echap04_vol1.pdf.

19. *Bulk Data Sharing Policy and Procedure*, op. cit.

20. Ibid.

21. Dave Maas and Aaron Mackey, "California's Sensitive Law Enforcement Databases Were Violated in 143 Cases Last Year," *Electronic Frontier Foundation*, 20 June 2018, accessed 31 August 2019, https://www.eff.org/deeplinks/2018/06/clets-misuse-2017.

22. Dave Maas, "Misuse Rampant, Oversight Lacking at California's Law Enforcement Network," *Electronic Frontier Foundation*, 18 November 2015, accessed 31 August 2019, https://www.eff.org/deeplinks/2015/11/misuse-rampant-oversight-lacking-californias-law-enforcement-network.

23. Richard G. Greenleaf, Arthur J. Lurigio, Jamie L. Flexon and Teri J. Walker, "Race-based Decisions: Traffic Citations and Municipal Court Dispositions," *Justice Policy Journal* 8, no. 1 (2011), accessed 31 August 2018, http://www.cjcj.org/uploads/cjcj/documents/Race-based_decisions.pdf.

24. Williams, Betsy Anne, Catherine F. Brooks and Yotam Shmargad, "How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications," *Journal of Information Policy* 8 (2018): 78–115.

25. Justice K.S. Puttaswamy vs. Union of India and Ors, The Supreme Court of India, 24 August 2017, accessed 29 August 2019, https://sci.gov.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.

26. The Personal Data Protection Bill, 2018, Ministry of Electronics and Information Technology, accessed 29 August 2019, 5, https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

27. Ibid.

28. Paul Lewis, David Pegg and Alex Hern, "Cambridge Analytica kept Facebook data models

through US election," *The Guardian*, 6 May 2018, accessed 31 August 2019, https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election.

29. Bruce Biegel, Jonathan Margulies, Gina Maggi and Chloe Davis, *The State of Data*, The Winterberry Group in Partnership with Interactive Advertising Bureau, 5, https://www.iab.com/wp-content/uploads/2018/12/IAB_The-State-of-Data-2018_2018-12-05_Final.pdf.

30. Jeffery Dastin, "Amazon offers $10 to Prime Day shoppers who hand over their data," *Reuters*, 16 July 2019, accessed 31 August 2019, https://www.reuters.com/article/us-amazon-com-prime-day/amazon-offers-10-to-prime-day-shoppers-who-hand-over-their-data-idUSKCN1UB164.

31. IANS, "Cashback incentives to push Google Pay in India," *Livemint*, 17 May 2019, accessed 31 August 2019, https://www.livemint.com/technology/apps/cashback-incentives-to-push-google-pay-in-india-1558085276436.html.

32. Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30 (2015): 75–89, accessed 31 August 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754.

ORF OBSERVER RESEARCH FOUNDATION

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000 Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org