NLSIR

GSTN- THE NEW NETWORK

—Karthik Sundaram*

Abstract A robust IT infrastructure holds the key to the successful implementation of GST in India. Much like the GST scheme, the GST Network has also been the subject of much critique. The author in this article discusses two major concerns that have been voiced with the structure of the GSTN. First, the structure and functioning of the GSTN as a NIU has been discussed along with the possibility of interference by non-governmental bodies. Second, the author has dealt with the privacy concerns emerging from such a large scale collection of data by GSTN. This has been analysed in the backdrop of the debate surrounding whether the right to privacy is a fundamental right at all. The article concludes with suggestions on how these two concerns could be best addressed without compromising on the effectiveness of the GSTN.

I. INTRODUCTION

After a long and arduous journey, the efforts towards implementation of the Goods and Services Tax (hereinafter 'GST') regime in India have borne fruit, and India will see the implementation of GST in 2017. Per the terms of the Constitution (101st Amendment) Act which has amended the Constitution of India w.e.f. 16th September, 2016, GST is required to be implemented latest by 16th September, 2017. GST is expected to be a transformational change in the indirect tax landscape of India; the introduction of which is greatly expected to benefit the Indian economy.

GST seeks to facilitate the development of a common national market in India. Thus, the backbone of administration of the GST regime by the tax authorities will be the GST related information technology infrastructure, which seeks to integrate all transactions on a pan India basis, to facilitate an integrated tax administration at both the central and state level.

* The author is an advocate in the Madras High Court specialising in the area of taxation law.

It is in this context that the present article seeks to discuss the need and basis for setting up the GST Network (hereinafter 'GSTN'), which will in turn set up and provide the IT backbone for the effective functioning of the GST regime. Since the GSTN is a Section 25 company[1] set up as a 'public-private partnership' and the GSTN will have access to a significant amount of tax related data relating to individuals, businesses and companies, some 'right to privacy' issues have also been raised in such context.

In addition to the above, various concerns have also been raised as regards the shareholding pattern of the GSTN, and the role of private entities as stakeholders in GSTN. Some concerns have also been raised as to whether a security clearance from the Ministry of Home Affairs is required for private entities which are a part of GSTN. Issues have also been raised by the Department of Revenue and the Department of Expenditure in the Ministry of Finance on the constitution of the GSTN, the expenses incurred by the GSTN, and whether the GSTN can actually be managed more effectively by the Central Board of Excise and Customs (hereinafter 'CBEC'), or other departmental bodies.[2] The Select Committee on non-government shareholding of GSTN by private banks had in fact recommended that the Government take steps to ensure that non-governmental financial institution shareholding be limited to public sector banks or public sector financial institutions given that: (i) public sector banks have more than 70% share in total credit lending in India; and (ii) GSTN's work is of strategic importance to the country and that the firm would be a repository of sensitive data on business entities across the country.[3]

This article primarily seeks to deal with the thought process behind setting up the GSTN and the issues relating to data security and the right to privacy.

II. SETTING UP OF NATIONAL INFORMATION UTILITIES AND OF GSTN AS A NATIONAL INFORMATION UTILITY

The then finance minister in his budget speech of 2010–2011 had announced the setting up of a Technology Advisory Group for Unique Projects (hereinafter 'TAGUP'). As conceived by the TAGUP, National Information Utilities (hereinafter NIU) would be private companies with a public purpose. Although companies would be profit-making, they would not have a profit maximising objective. As conceived, an NIU would make available essential infrastructure for public service. It was thought that such institutions would make it possible for government

---

1 Registered under Section 25 of the Companies Act, 1956.

2 *DoE red flags large expenditure by GST-Network*, THE INDIAN EXPRESS, (June 26, 2016), http://indianexpress.com/article/india/india-news-india/doe-red-flags-large-expenditure-by-gst-network-2876711/ (July 6, 2016).

3 Sumit Dutt Majumder, GST IN INDIA 419-420 (2nd ed., 2016).

functions to be carried out efficiently, and allow feasible projects to be designed, thus fostering economic development. Like public-private partnerships in the infrastructure space, NIUs as conceived, are to function in a manner so as to have a net positive effect on society. The idea itself is not a new one, although the concept of NIUs has been further developed. Successful examples in the Indian context itself exist in the form of National Security Depository Limited, National Payments Corporation of India, and the Centre for Railway Information Systems.

The NIUs have been envisaged to be primarily responsible for technology-related aspects of implementation. They are bound by tight service level agreements, and are subjected to periodic audits. The NIUs would be designed in a manner so that strategic control is retained with the government at all times. To facilitate this, it was decided that no single private entity would own more than 25% of the shares in an NIU, and that institutions which have a direct conflict of interest (such as, IT companies) would not be permitted to be shareholders. The TAGUP had also recommended that the Government-NIU relationship should be defined through an agreement which would outline the broad project goals, placement of tasks, financials, service level agreements, and most importantly, embody the spirit of partnership. The agreement as contemplated covers the following specific areas – (a) scope of work; (b) activities to be undertaken by NIUs; (c) obligations of the government and NIUs; (d) financial arrangement; (e) service level agreement; and (f) business continuity plan upon exit.

It was in this backdrop that the Information Technology Group of the Empowered Committee of Finance Ministers on GST recommended that the GSTN be set up as a NIU for managing the IT systems for GST implementation, including the Common GST Portal. Therefore, much thought and deliberation has gone into setting up of the GSTN as an NIU for the effective implementation of GST in India.

III. THE CONSTITUTION AND FUNCTIONS OF GSTN

The GSTN has been set up as a Section 25 not-for-profit company, in which the Government of India and State Government hold 49% of the shareholding, and the balance 51% is held by corporations and banks such as LIC, ICICI, HDFC etc. In line with the recommendations of the TAGUP, no software company has any shareholding in GSTN.

GSTN has been set up as a company to primarily provide IT infrastructure and services to the central and state governments, tax payers and other stakeholders for implementation of GST. The key work of GSTN will be to:

a) provide common registration, return, and payment services to the tax payers;

b) partner with other agencies for creating an efficient and user-friendly GST eco-system;

c) encourage and collaborate with GST Suvidha Providers to roll out GST applications for providing simplified services to the stakeholders;

d) carry out research, study best practices, and provide training and consultancy to the tax authorities and other stakeholders.

e) provide efficient backend services to the tax departments of the central and state governments on request;

f) develop Tax Payer Profiling Utility for central and state tax administration;

g) assist tax authorities in improving the tax compliance and transparency of the tax administration system; and

h) deliver any other services of relevance to the central and state governments and other stakeholders on request.

The common GST portal is to be a pass-through device for information, while enhancing it with intelligence to plug leakages. It would also act as a tax booster, matching the input tax credits in the returns to detect tax evasion. It can also integrate with various other systems at Ministry of Corporate Affairs and Central Board of Direct Taxes for verification of PAN or other corporate information, and perform data mining and pattern detection to detect tax fraud. It would send this information as alerts and reports to the respective tax authorities. It would also compute inter-state settlement, netting IGST across states.

If one looks at the Central GST ('CGST')/State GST ('SGST') enactments, it is clear that 'Input Tax Credit' (hereinafter 'ITC') related records will be required to be maintained on an electronic credit ledger. The ITC can be availed by the purchasing dealer only subsequent to payment of GST by the selling dealer. The GST system will be designed to capture mismatches between the records of the selling dealer and the purchasing dealer. It will ensure that all taxes are fully paid, and there are no leakages in tax revenue, and that the ITC is allowed only after full payment of taxes to the respective governments. Thus, the fulcrum of GST will be the IT infrastructure since all registrations, returns and records are required to be maintained in electronic form. Hence, the GSTN is significant in the scheme of a successful GST.

IV. GSTN AND THE RIGHT TO PRIVACY

With the debate surrounding the introduction of GST in India, the setting up and functioning of the GSTN has also been subject to much critique. In some quarters the structure and functioning of the GSTN is viewed with circumspection, as it creates a basis for the storage of a large quantum of tax and other

related financial information with non-governmental parties. This creates a potential for misuse of such data and concerns regarding invasion of the right to privacy.

In this part of the article, the author seeks to address the issue of the actual contours of the right to privacy in India, and how it will play out in the context of functioning of the GSTN.

V. WHETHER THE RIGHT TO PRIVACY IS A FUNDAMENTAL RIGHT

The issue of whether the right to privacy is a fundamental right or not as guaranteed under the Indian Constitution has been referred to a larger bench of the Supreme Court for consideration in *K.S. Puttaswamy v. Union of India*.[4] While making such reference, the Supreme Court has observed that it is better that the *ratio decidendi* of *M.P. Sharma v. Satish Chandra*[5] and *Kharak Singh v. State of U.P.*,[6] is scrutinized, and the jurisprudential correctness of the subsequent decisions of this Court where the right to privacy is either asserted or referred be examined and authoritatively decided by a bench of appropriate strength. Both *M.P. Sharma* case and *Kharak Singh* case, which were decisions rendered by a 8 judge bench and 7 judge bench of the Supreme Court respectively, were rendered in the context of issues such as power of search and seizure and police regulations dealing with domical visits. Both have held that the right to privacy is not a fundamental right under the Indian Constitution. Albeit rendered by smaller benches, later decisions of the Supreme Court such as *Gobind v. State of M.P.*,[7] *People's Union for Civil Liberties (PUCL) v. Union of India,* [8] and *R. Rajagopal v. State of T.N.*,[9] (wherein the Court had for the first time linked the right to privacy to Article 21 of the Constitution), have taken the view that the 'right to privacy' is a fundamental right under the Indian Constitution. In fact, in *District Registrar and Collector v. Canara Bank*,[10] the Supreme Court struck down a provision of the Andhra Pradesh Stamps Act which allowed the collector or 'any person' authorised by the collector to enter any premises to conduct an inspection of any records, registers, books, documents in the custody of any public officer, if such inspection would result in discovery of fraud or omission of any duty payable to the government, by holding that it failed the tests of reasonableness enshrined in Articles 14, 19 and 21 of the Constitution (including the right to privacy of a citizen *qua* his financial records).

---

4 *K.S. Puttaswamy* v. *Union of India*, (2015) 8 SCC 735.

5 *M.P. Sharma* v. *Satish Chandra*, AIR 1954 SC 300.

6 *Kharak Singh* v. *State of U.P.*, AIR 1963 SC 1295 : (1964) 1 SCR 332.

7 *Gobind* v. *State of M.P.*, (1975) 2 SCC 148 : (1975) 3 SCR 946.

8 *People's Union for Civil Liberties (PUCL)* v. *Union of India*, (1997) 1 SCC 301.

9 *R. Rajagopal* v. *State of T.N.*, (1994) 6 SCC 632.

10 *District Registrar and Collector* v. *Canara Bank*, (2005) 1 SCC 496.

Therefore, there are conflicting Supreme Court decisions on the issue of whether or not the right to privacy is a fundamental right under the Indian Constitution. While the more recent decisions of the Supreme Court take a view that such 'right to privacy' is indeed a fundamental right, the conflict on the correct legal position will be resolved only when the larger bench of the Supreme Court answers the reference made in *K.S. Puttaswamy.*

Various jurisdictions across the globe have well articulated privacy policies which spell out the requirements for protection of personal data, and prevent harm to an individual whose data is at stake. In the Indian context, the report of the group of experts on privacy[11] (hereinafter 'the Report') headed by Former Justice A.P. Shah which was presented in October, 2012 had set out various recommendations for consideration by the government while formulating the proposed framework for a Privacy Act. The Report is premised on the fact that right to privacy has emerged and evolved as a fundamental right through various Supreme Court decisions, while this position is itself in question before the Supreme Court in *K.S. Puttaswamy.* In fact, the 2014 version of the Right to Privacy Bill which has still not been enacted, proceeds on the presumption that the right to privacy is a fundamental right guaranteed under Article 21 of the Constitution of India.

Therefore, to put it succinctly, the position as regards the right to privacy in India is as under:

- There are conflicting Supreme Court decisions on whether the right to privacy is indeed a fundamental right, and the matter is pending decision before a larger bench of the Supreme Court;
- Though the government has sought to enact a Right to Privacy Act which will statutorily provide for such right, exceptions to the right of privacy, situations where access to data with authorization will not constitute an invasion of the right to privacy, and offences and consequential penalties, the proposal is still at the stage of a Bill of Parliament and has not seen the light of the day.
- In terms of the extant legislation, only the Information Technology Act, 2000 (hereinafter 'IT Act') contains some provisions regarding data protection as opposed to data privacy. For instance, Section 43A of the IT Act provides that "*where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages by way of compensation to the person so affected.*" Further section 73A also provides for penalties

[11] Planning Commission, Report of the Group of Experts on Privacy (2012).

including imprisonment for wilful disclosure of personal informational secured under a lawful contract without authorization of such person disclosing the information, or in breach of such lawful contract.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, provides for detailed rules as regards the security practices and procedures related to sensitive personal data or information. The term 'sensitive personal data or information' as defined under Rule 3 of the said Rules does not appear to cover tax related information.

Therefore the IT Act and the rules framed thereunder though it contains provisions related to data protection are not geared to protect the use of tax related information.

The right balance between the individual's right to privacy and the larger public interest should be achieved by the data protection framework. While personal information relating to the individual must be strictly protected from unauthorized access, there may be a need for government agencies to access or share this data for purposes of national security, economic offenses, tax evasion and other specified circumstances. Hence, authorized sharing of information under specified circumstances *ipso facto* should not be considered as a violation of an individual's right to privacy. However, detailed processes, systems, and guidelines need to be put in place to ensure that authorized access and sharing is within the parameters set by law.

VI. VIEWS OF THE EMPOWERED COMMITTEE ON DATA SECURITY IN THE CONTEXT OF GSTN

The EC has not been unaware of the concerns surrounding data security. The issue has been examined by the EC while deciding the final structure of the GSTN. The suggestions/clarifications given by EC on data security are as under:

- provisions regarding data security will be addressed by incorporating related provisions in the Articles of Association of the company entrusted with GSTN.
- the Chairman of the GSTN will be appointed by the government and no single private entity will own more than 10% of equity, while the Centre and the States will own 24.5% equity each. Thus, ultimate control will vest with the government.
- the GSTN will be bound to follow the internationally accepted security and safety measures for preventing data leakage. A proposal was also mooted to appoint a chief information security officer on deputation by the government to look into the matters related to information security.

- audits of GSTN would be conducted by the independent auditors, including the professional personnel designated for carrying out technology reviews and giving suggestions thereupon.
- an overarching IT security management framework comprising Plan-Do-Check-Act (PDCA) cycle to be employed to ensure data security and confidentiality.[12]

VII. RECOMMENDATIONS OF THE TAGUP ON DATA SECURITY

The TAGUP in its report dated 31st January, 2011 has made certain recommendations regarding data protection in the context of NIUs, which may serve as useful guidelines for designers of IT systems till such time as a formal legislation on privacy is passed. Some of the recommendations are enumerated below:

- The solution architecture of a project should be designed for data protection and privacy from the ground up.
- The privacy framework for a project should be defined early on, which transforms the legislation on privacy into implementable rules for IT systems.
- The design of the solution architecture should ensure that any Personal Identifiable Information (PII) is stored safely, and that access is carefully monitored. Stringent penalties must be in place to address the issue of unauthorized access of personal data by outside agencies as well as by personnel within the organization. Strict protocols and processes must be in place to detect such access in order that they are dealt with swiftly and in a deterrent manner. This is not only desirable from a privacy perspective, but also from a security perspective.
- Anonymization of data is an important aspect of privacy. Data should be carefully anonymized when released publicly, or when shared with other organizations that do not require access to PII, as allowed within the data protection and privacy framework.
- Careful thought should be given to anonymization, since naive approaches to deidentifying data are prone to attacks that combine the data with other publicly available information to re-identify individuals.
- Data retention and usage policies should be well-defined, especially for PII. In case the legal framework of the project provides for it, an individual should be able to access data stored in the IT system about themselves, after appropriate authentication of their identity.

[12] Sumit Dutt Majumder, *supra* note 3, at 408.

- The right balance between the individual's right to privacy and the larger public interest should be achieved by the data protection framework. While personal information relating to the individual must be strictly protected from unauthorized access, there may be a need for government agencies to access or share this data for purposes of national security, economic offenses, tax evasion and other specified circumstances. Hence, authorized sharing of information under specified circumstances, ipso facto, should not be considered as a violation of an individual's right to privacy. However, detailed processes, systems and guidelines need to be put in place to ensure that authorized access and sharing is within the parameters set by law.

The design of GSTN is based on "role based access." The taxpayer can access his own data through identified applications like registration, return, view ledger, etc. The tax official having jurisdiction as per the GST law as well as the audit authorities can access the data. No other entity can have any access to the data on GSTN.[13]

VIII. CONCLUSION

While there has been some thought and effort on ensuring 'data security', ensuring the right to privacy though the issue whether it is in the nature of a fundamental right or will remain a statutory right remains open at this time, much more requires to be done. Further, on the issue of balancing the right to privacy with larger public interest, mere policy guidelines/statements without a substantive statutory framework cannot achieve the desired result. Mere policies cannot guarantee rights or ensure their enforcement.

Given the importance of the GSTN as an NIU, and the role which NIUs may play in the future given the digital transformation of India, it is the suggestion of the author that it is important that the setting up and functioning of NIUs be governed by a statutory framework specific to NIUs. The government should consider the introduction of a comprehensive legislation specific to NIUs which could *inter alia* contain provisions on issues such as, setting up and constitution of NIUs, shareholding pattern, data security, right to privacy, exceptions thereto and enforcement thereof, co-relation between right to privacy and larger public interest, sharing of tax and other information between government agencies, etc. A statutory framework would not only guarantee rights but also enable enforcement of the same, as a right without a remedy is but no right at all.

[13] GOODS AND SERVICES TAX NETWORK (March 25, 2017, 8:00 PM) http://www.gstn.org/index.php/about-us#concern.