Smart Cities: Need for a regulatory framework

Introduction

The Smart Cities Mission ("**Mission**") aims to develop 100 smart cities by 2020. It is one of the most ambitious programmes of the Indian government. To implement its objectives, the government introduced the Smart Cities Guidelines ("**Guidelines**") in 2015.[1] The Guidelines act as a comprehensive policy document that defines smart cities as cities that interconnect citizens, data, devices and objects to a centralised network infrastructure which will be utilised for urban planning, social and economic development of the city and its citizens. Smart cities will rely on information communication infrastructure and data (defined as information, knowledge, facts, concepts or instructions processed in a computer system or computer network) for its service delivery mechanisms. While the Guidelines provide for a clear strategy on the implementation of this Mission, both at the state and city level, it is completely silent on the legal framework required thereof. Though the government has introduced various draft policies for the smooth transition into smart cities, these are yet to be implemented into laws that can govern the Mission.

This newsletter attempts to highlight the inadequacy of the current regulatory framework with regard to technology laws and smart cities.

1. Smart city implementation and challenges

The smart city projects will be implemented at the city level through Special Purpose Vehicles incorporated as limited companies under the Companies Act, 2013. They will be responsible for the project appraisals, approvals, release of funds, implementation, evaluation and monitoring.

One of the key concerns with regard to the execution of the Mission arises from the public private partnerships in project execution. . While the government will contribute a substantial amount to finance these projects, it is estimated that the Mission will require about USD 150 billion[2] investment from the private sector.[3] These investments will be in the development of sophisticated technologies such as Internet of Things ("**IoT**"), which refers to a network of objects and devices connected through the internet and Machine to Machine ("**M2M**"), i.e., communication between devices or machines through wireless and wireline networks. This raises concerns of privacy, data sharing, protection of sensitive personal information, cyber hacking, identity theft etc. The National Telecom Policy, 2012, which is the overarching guiding policy for telecommunication and technology in India, includes IoT and M2M technologies as new technologies that improve public welfare and offer tremendous

[1] See "Smart Cities Mission Statement and Guidelines" available at http://smartcities.gov.in/writereaddata/smartcityguidelines.pdf (last accessed on Jan 20, 2017)
[2] 1 USD = about INR 68
[3] See "Over $150 billion investments required for smart cities: Deloitte", The Economic Times (Feb 03,2016) available at http://economictimes.indiatimes.com/articleshow/50791945.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last accessed on Jan 16, 2017)

growth opportunities. In light of this, the Ministry of Electronics and Information Technology of India released a policy document for IoT and M2M technologies along with a National Cyber Security Policy, 2013. It is noteworthy that none of these policies have been implemented by the government yet. Prior to roll-out of project proposals, the government would need to ensure a stable and predictable regulatory environment including a re-visit of information technology laws.

2. The legal framework (or lack of it)

Below is a high-level summary of the current legislations and how they are not equipped to handle the challenges that are likely to come up.

2.1 The Information Technology Act

The Information Technology Act ("**Act**") governs the scope of internet activity in India. The Act was implemented to provide legal recognition to electronic transactions, validate digital contracts and regulate online services. The development of smart cities will witness different entities dealing with networks, designs, software, manufacturing of devices, etc. There will also be a surge in "Big Data" i.e., enormous sets of unstructured data analysed computationally to understand patterns relating to human behavior. Currently, the term "data" under the Act is defined as representation of information, knowledge, facts, concepts or instructions being prepared in a formal manner and processed in a computer system. Clearly, the definition does not consider the implications of Big Data which comprises of varied sets of data which will be stored and processed by government(s), private organisations and individuals. The rise in Big Data would pose new security challenges relating to personal information and privacy. Further, the term "cyber security", which is defined as protecting information, equipment, devices, computer resource from unauthorised access, disclosure, disruption, modification and destruction must be adaptive to the evolving nature of security risks as the advent of smart cities could lead to criminal activities that are beyond the scope of the current definition. This calls for a reexamination of the current provisions under the Act.

2.2 National Cyber Security Policy, 2013

To address the present lacuna of laws to tackle cybercrimes, the government introduced the National Cyber Security Policy, 2013[4] ("**Policy**") which recognises cyber space as a critical sector and aims to build security mechanisms at national and sectoral levels. The Policy recommends (a) establishment of a National Critical Information Infrastructure Protection Centre responsible for mandating security practices related to design, acquisition, development and use of information, (b) a nodal agency to coordinate all matters of cyber security, (c) to designate a Chief Information Security Officer, to lead the internal security measures in organizations, (d) encourages collaboration between the government and private sector to enhance open standards for certified IT products, (e). jointly develop a cyber security framework with other countries that recognises the applicability of international law and the UN Charter. The Policy, expected to be implemented in a phased manner, also provides

[4] See http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf (last accessed Jan 20, 2017)

economic schemes and incentives to organizations for strengthening their cyber security information infrastructure, including global security best practices.

2.3 E-Governance and the Right to privacy

The Act recognises e-governance by providing legal sanctity to digital signatures, electronic service delivery and retention of electronic records. Sharing and exchange of information between government and private parties will be at the core of the Mission. Presently, the Act does not address the risks associated with this and it remains a grey area.

Right to privacy is a constitutional right, yet the Act is inadequate as the provisions are confined to the protection of sensitive personal data under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011("**Rules**"). These Rules regulate private entities and exclude the government from its ambit. The Act and Rules define "personal information" as information relating to a natural person and excludes real-time data i.e., data collected and processed by different applications, to relay information without any delay in timelines.

Smart cities would involve communication among devices with little or no human intervention. Services will be delivered over networks on real-time basis to be used for differing purposes. The current Rules require a body corporate to obtain consent in writing to collect data from the provider of sensitive personal data. The variety and the velocity of data exchanged in the context of smart cities will make this an unfeasible exercise.

Currently, India does not have a comprehensive privacy policy governing the conduct of different stake holders engaged in the information technology chain. Privacy matters are also governed by Contract Act, 1872 and are included as boiler plate clauses in various agreements signed by application, service providers and network providers to the end users. For example, every website has a policy on privacy incorporated in it, seeking consent of the user for collection and retention of information as well as a separate policy outlining the manner in which the information is intended to be used by the collector. The absence of a regulation creates an atmosphere of uncertainty leaving various private entities to decide information that is critical depending on the business risk.

2.4 IoT policy

The draft policy predicts the impact of IoT across different sectors, but does not mention a regulatory framework to tackle the associated risks. Since IoT relies on the communication between devices through the internet networks, there may be instances of unauthorised access and misuse of personal information. IoT devices may facilitate attacks on other systems and create risks to personal safety. Privacy risks may also flow from the collection of personal information. The present Act does not consider the collection and use of real-time data as part of personal information, thus, affording little or no protection to exposed users. The draft policy reveals the government's intention to (a) focus on research and development to further the progress of IoT, (b) promote venture funds which will aid and support entities working in IoT related domains by providing 100% duty benefit for imported raw materials for manufacturing IoT products; and (c) support and encourage manufacturing of IoT devices

supporting the government's "Make in India" campaign. All of this is, again, yet to be implemented.

2.5 Geospatial Information Regulation Bill, 2016

The Ministry of Home Affairs released the first draft of India's Geospatial Information Regulation Bill, 2016 ("**Bill**"). The Bill intends to regulate citizens, private and foreign entities, involved in the acquisition, dissemination, publication and distribution of geospatial information through a licensing framework.[5] The Bill defines, *"Geospatial Information" to mean geospatial imagery or data acquired through space or aerial platforms such as satellite, aircrafts, airships, balloons, unmanned aerial vehicles including value addition; or graphical or digital data depicting natural or man-made physical features, phenomenon or boundaries of the earth or any information related thereto including surveys, charts, maps, terrestrial photos referenced to a co-ordinate system and having attributes"* Thus, it seeks to regulate information collected by private entities on the basis of threat to the national security and sovereignty. This may cause adverse impact on application service providers that collect real time data for the provision of services. The Bill seeks to protect citizens from unauthorised collection and use of individual information by private entities only,[6] thus excluding the government.

The Bill states, any person (natural and legal) involved in the acquisition of geospatial information or data would need to apply for a license. Once passed, the Bill may impact most application service providers, software providers, network companies, discouraging either the domestic innovation of such applications or paving an exit for foreign entities operating in India. Considering the intent of the Bill is to safeguard national security, policymakers would need to find a middle ground where regulation does not impede technological progress.

Conclusion

Since there are no laws governing smart cities specifically, the government will have to amend current laws to align with the objectives of the smart city program. In time to come, it may be essential to examine the feasibility of developing a comprehensive law on cyber security, privacy, data protection and standardization of equipments. This can be done through amendments in the Act or a new set of rules that address the aforesaid challenges. The success of the foregoing programme will depend on the underlying telecommunication infrastructure which is a capital-intensive industry, requiring strong collaboration between governments and private entities. In this light, it is essential that the legislature and policymakers develop clarity in the present regulations to evoke investor confidence.

Author
Arijita Kakati

[5] See Draft Geospatial Information Regulation Bill, 2016, available at http://mha.nic.in/sites/upload_files/mha/files/GeospatialBill_05052016_eve.pdf (last accessed on Jan 20, 2017)