Information Technology Industry Council (ITI) Comments on TRAI's Consultation Paper on M2M Communications

January 3rd, 2017

ITI[1] appreciates the opportunity that the Telecommunications Regulatory Authority of India (TRAI) has provided for submitting public comments on the recently issued *Consultation Paper on Spectrum, Roaming, and QoS Related Requirements in Machine-to-Machine (M2M) Communications* (Consultation Paper No. 21/2016). ITI acknowledges and is grateful for TRAI's consistency in issuing high quality public consultation documents that address many of the most complex and important issues that new technologies present. In addition, ITI applauds TRAI's initiative in considering the potential policy challenges that M2M communications may present for the government. ITI's comments in response to this consultation document will focus on the privacy and security aspects of M2M communications. Our comments also explain why the free flow of data is critical to the success of this digital technology.

Q12. *Will the existing measures taken for security of networks and data be adequate for security in M2M context too? Please suggest additional measures, if any, for security of networks and data for M2M communication.*
-and-
Q13. *(a) How should the M2M Service providers ensure protection of consumer interest and data privacy of the consumer? Can the issue be dealt in the framework of existing laws?*
(b) If not, what changes are proposed in Information Technology Act. 2000 and relevant license conditions to protect the security and privacy of an individual?

TRAI is right to be concerned about M2M security and privacy; the recent and continuing proliferation of devices and sensors is also increasing points of vulnerability. The Government of India (GOI) can take important steps to ensure that India's M2M ecosystem is secure while enabling it's M2M industry to grow and compete in the global market.

First, strong encryption is fundamental to M2M security and consumer privacy. Though not fully sufficient on its own, ensuring that data is encrypted both when it is being stored and while M2M devices are communicating over the internet is the first step in device and network security. As such, the GOI should resist urges to require backdoors or other mechanisms that weaken encryption for users and businesses alike and encourage companies to utilize the most up-to-date encryption software and practices.

TRAI should consider creating a cybersecurity framework similar to those that are currently in use in both the United States and Italy. These frameworks create a common language for companies, governments, and NGOs to counter cybersecurity threats collaboratively through voluntary, internal standards. The framework approach leverages public-private partnerships and is effective because it allows flexibility for dynamic and rapid responses to existing and emerging threats, grounded in effective risk management while acknowledging the global, interconnected nature of these systems. This broad, holistic approach to

[1] The Information Technology Industry Council (ITI) is the global voice of the tech sector, celebrating its 100th year in 2016 as the premier advocacy and policy organization for the world's leading innovation companies. In both the U.S. and in countries around the world, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more and follow us on Twitter for the latest ITI news @ITI_TechTweets.

securing the ecosystem across the supply chain rather than targeting one producer or supplier via regulation is effective at securing all systems by understanding that M2M is a part of the broader internet ecosystem. It does this by acknowledging that the network layer, device layer, and software layer all play a role in security and thus require a multipronged approach.

Consumer education and awareness is another critical point of engagement for governments. Through consumer education, a market-based incentive to differentiate products based on security features will have a positive impact along the supply chain. TRAI also should consider incentivizing small and medium-sized enterprises (SMEs) to create products and systems that are patchable and upgradable so that they can effectively compete and grow in the M2M market without compromising the security of the network. TRAI should encourage all companies to design security into their systems from the ground up, and to connect thoughtfully. To enable this, TRAI can release guidance to SMEs and under-resourced manufacturers, which encourages the use of internationally recognized security standards and best practices.

Regarding the IT Act, ITI advocates that it should explicitly highlight the importance of strong encryption and disallow any company from being compelled to introduce a vulnerability into their product. In addition, the IT Act currently puts forth data retention requirements on certain service providers. While this is done with the legitimate goal of helping law enforcement and governments assure national security, the downfall is that compelling mass retention of data creates additional risk and attack surfaces. Therefore, data retention and storage should be time-limited and targeted in scope. Requiring the storage of massive data sets creates more security risks and imposes greater costs on companies to secure that data. This can compromise the integrity and overall security of the entire ecosystem. Please see ITI's response to Q16 for additional views on data localization requirements and restrictions on cross-border data flows.

The key to effective security and privacy regulations is to avoid over-regulation; there are many market mechanisms that encourage companies to secure their systems and devices. Therefore, TRAI's role should be to encourage and enable, rather than require, companies to build security into their products, in turn creating both a secure and dynamic technology sector within India.

Q16. *Please give your comments on any related matter not covered in this consultation paper.*

ITI would like to emphasize the importance of enabling cross-border data flows and avoiding forced data localization when considering how to best regulate M2M technologies. The consultation document expresses concerns regarding the security of data based on where the data is stored and processed. These are legitimate concerns, and TRAI is justified in considering how the location of data, and transmission of that data, may or may not affect its security. However, forced local storage of data will have a significant impact on the cost and availability of M2M services, dampening the potentially transformational benefits of M2M products for manufacturing, technology companies, and consumers. In addition, data localization does not provide meaningful security benefits to data, degrading the justification for forced local storage.

Mandating local storage of data increases costs for companies. Data storage and processing relies on the economies of scale that can be found in large data centers. Companies, even very large multinational companies, use very few facilities for their global data processing needs. This allows them to provide

effective low costs, high quality services. Mandating that this process take place within certain borders can raise the cost for companies to procure data services by 30-60%.[2] Not only is this cost crippling for SMEs, it translates to massive macroeconomic costs: economy-wide data localization in India could cost up to .8% of its GDP and decrease investments by 1.3%, causing economy-wide welfare losses per worker equivalent to 11% of the average monthly salary.[3] The result of these large costs includes a dampening of M2M adoption and would be a significant challenge for India firms to overcome in order to compete in the global economy.

Given this large economic cost, TRAI should consider trade and investment friendly policy tools other than data localization to secure their systems, protect privacy, and provide law enforcement access to data. This submission already touched on ITI's views for privacy and security, but TRAI is justifiably concerned about the ability of India's law enforcement to enforce its laws when needed data is stored outside the borders of India. However, India should focus on strengthening its Mutual Legal Assistance Treaties (MLATs) and similar mechanisms for international law enforcement assistance instead of mandating data localization. In instances where companies are storing particularly sensitive data, they can determine additional security measures, including where data is stored, at the contract level. Restrictive, overly general requirements for local storage of data will negatively impact the Indian economy. Security of, and access to, data can be achieved without it.

[2] "Quantifying the Cost of Forced Localization" Leviathan Security Group, 2015.
[3] "The Costs of Data Localisation: Friendly Fire on Economy Recovery" ECIPE, 2014.