No.: 97/TRAI/2016-17/ACTO
Dated: 5th July, 2016

Shri A. Robert J. Ravi
Advisor (QoS)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi - 110 002

Ref: **ACTO Response to TRAI's Pre Consultation on Net Neutrality dated 30th May, 2016**

Dear Sir,

We express our sincere thanks to the Hon'ble Authority for bringing this pre consultation paper on Net Neutrality.

ACTO is pleased to provide its responses to the issues posed in the captioned Consultation Paper.

We hope that our comments (enclosed as Annexure – I supported with Annexure II) will merit the kind consideration of the Hon'ble Authority.

Respectfully submitted,

Yours sincerely,

for Association of Competitive Telecom Operator

Tapan K. Patra
Director

Encl: As above

ANNEXURE-I

ACTO Comments on TRAI Pre-Consultation on Net Neutrality May 30 2016

Background

ACTO appreciates the opportunity to express its views in this Pre-Consultation and hopes that these comments will be helpful to the Authority in examining the issue of Net Neutrality and in formulating its views on the path forward that best promotes the principles of an Open Internet. We believe the TRAI can preserve Internet freedom and openness, and that it can do so without over-regulation so as to enhance broadband investment and deployment. We consider the opening of this Pre-Consultation to be an opportunity for the TRAI to build a regulatory framework to define its authority in a way that promotes the free flow of Internet-based content and services, with a view to promoting the deployment of broadband and the sustainable development of the Information Society.

General Comments

At the outset, we emphasize that our members are committed to the goal of maintaining an Open Internet policy that promotes an ecosystem where users are able to freely exchange ideas and communicate, to access the applications and legal contents that they wish to use, and to select the service packages that best satisfy their needs. However, a key factor for promoting the growth and availability of the Internet and in reaching the objectives of the Digital India program consists in avoiding unnecessary regulations that discourage investments in infrastructure and services, distort competition among operators, and limit the possibility for the users to choose offers that meet their needs and ability to pay.

ACTO endorses the policy and principles of an Open Internet, which to us means an entire Internet ecosystem that enables users to exchange ideas and communicate freely, gives them freedom to access the lawful applications and content they wish to use, and affords them the ability to choose and assemble packages of services and equipment that meet their needs.

When supporting an Open Internet, ACTO is guided by the following core standards/ principles in addressing the needs of our customers in approaching new Internet-related business opportunities, designing new services, and managing our network:

- **Freedom** – Consumers should be able to openly exchange ideas, content, and information across the Internet.

- **Innovation** – Consumers are entitled to a robust and highly secure network that enables new services, applications, and devices.
- **Competition** – Consumers have the power to choose the best possible services and innovations.
- **Transparency** – Consumers should have clear and concise information about speed, cost, and traffic management.

In less than two decades, the Internet has evolved dramatically from being a network that provided only file downloads and remote access to distant academic or government computers, to being a vibrant global commercial network that now provides countless different services to millions of content and applications providers and billions of users. During the past decade, during a time when proponents of strict Net Neutrality regulation have raised dire warnings about the risk of broadband Internet access providers limiting choice and access, such Internet access providers instead have poured more than a trillion dollars into next-generation networks capable of providing advanced services. Over this decade, that network investment has paved the way for an entire Internet ecosystem that successfully manages a previously unimaginable diversity and volume of content, applications, and services delivered over these advanced networks. The Cisco Visual Networking Index: Forecast and Methodology, projects continued accelerated growth between 2015 and 2020 most notably in smartphone traffic as usage shifts from fixed to wireline and wireless devices and video streaming usage continues to soar.[1] Beyond these projections, further dynamic advances will continue to occur in response to future technological change and consumer demand, spurred on by new developments, including the Internet of Things, Software Defined Networks, and Big Data Analytics.

[1]Cisco Visual Networking Index: Forecast and Methodology, 2015–2020, (June 6, 2016), projections include: **Annual global IP traffic will surpass the zettabyte (ZB; 1000 exabytes [EB]) threshold in 2016, and will reach 2.3 ZB by 2020**. Global IP traffic will reach 1.1 ZB per year or 88.7 EB (one billion gigabytes [GB]) per month in 2016. By 2020, global IP traffic will reach 2.3 ZB per year, or 194 EB per month; **Smartphone traffic will exceed PC traffic by 2020**. In 2015, PCs accounted for 53 percent of total IP traffic, but by 2020 PCs will account for only 29 percent of traffic. Smartphones will account for 30 percent of total IP traffic in 2020, up from 8 percent in 2015. PC-originated traffic will grow at a CAGR of 8 percent, while TVs, tablets, smartphones, and machine-to-machine (M2M) modules will have traffic growth rates of 17 percent, 39 percent, 58 percent, and 44 percent, respectively. **Traffic from wireless and mobile devices will account for two-thirds of total IP traffic by 2020**. By 2020, wired devices will account for 34 percent of IP traffic, while Wi-Fi and mobile devices will account for 66 percent of IP traffic. In 2015, wired devices accounted for the majority of IP traffic at 52 percent; **Globally, mobile data traffic will increase eightfold between 2015 and 2020**. Mobile data traffic will grow at a CAGR of 53 percent between 2015 and 2020, reaching 30.6 EB per month by 2020. **Global mobile data traffic will grow three times as fast as fixed IP traffic from 2015 to 2020**. Global mobile data traffic was 5 percent of total IP traffic in 2015, and will be 16 percent of total IP traffic by 2020.

It is submitted that traffic management has always been employed by operators so that the Internet can function effectively, efficiently and successfully. The reasonable traffic management has been recognized & allowed by the other regulatory authorities worldwide, including in the United States, Canada and the European Union.. Furthermore, the need for service providers to have the flexibility to manage network traffic and performance has also been recognized by the report of the DoT Committee on Net Neutrality, which has recommended that reasonable traffic management practices may be allowed but should be "tested" against the core principles of Net Neutrality.

Additionally would also like to highlight that the DoT's Committee on Net Neutrality has very rightly recommended that the framework/ guidelines of Net Neutrality should not be applicable for Enterprise services provided by the TSPs.

As discussed in more detail below, Enterprise services are properly excluded. Enterprise users necessarily require that their traffic is managed in a specific way according to their business needs. Telecom operators have been offering managed data services to Enterprise customers for years, over their data connections and private IP infrastructure. It may be noted that, in the same way the reasonable network management has been recognized by regulatory authorities in other countries, so too has the exclusion of enterprise services been maintained.

ACTO believes that any Net Neutrality principles that are adopted should be equally applicable to all components of the internet eco-system and should create the environment to foster growth and innovation.

ACTO respectfully submit its responses to the Questions raised in the Pre-Consultation as below:

Q.No.1 What Should Be regarded as the Core Principles of Net Neutrality in the Indian context? What are the key issues that are required to be considered so that the principles of net neutrality are ensured?

ACTO's Response:

The Internet has become the most powerful communications medium and engine for economic growth ever, and has achieved this unprecedented growth without prescriptive regulation of the

Internet that would have locked in place certain specific technologies or business models. To the extent that any regulatory intervention is found to be necessary to protect the Open Internet, it can be effective if it:

- Is appropriately targeted and limited to the adoption of meaningful transparency requirements, and the prohibition of blocking, degrading or otherwise unreasonably disfavoring some Internet traffic over other Internet traffic;
- Does not restrict user-driven prioritization, which can enhance consumer welfare and is for essential for many enterprise applications, from banking, to emergency services, to streaming video;
- Does not apply to enterprise and specialized services;
- Is competitively and technologically-neutral and avoids duplicative and inconsistent regulation.

Beyond these core priorities to preserve an Open Internet, any more invasive and prescriptive Open Internet regulation is unnecessary and would reduce investment incentives for all operators that build and maintain the Internet networks.

Q.2. What are the reasonable traffic management practices that may need to be followed by TSPs while providing Internet access services and in what manner could these be misused? Are there any other current or potential practices in India that may give rise to concerns about net neutrality?

ACTO's Response:

Internet operators have used traffic management practices for their networks for many years, since this is necessary to assure the quality of the service that they offer to the users. We believe that the concern that the Internet network traffic management or the differentiation of products may cause discriminatory or anticompetitive practices does not have a certain basis and does not justify the imposition of strong regulatory burdens.

There is no incentive for the operators to degrade the quality of the services or impact their users, as the competitive pressure of the market prevents such conduct, given that it would generate a migration of customers towards rival operators that offer no restrictions. It is submitted that the TRAI should focus on network management practices only if there is evidence of an anti-competitive intent to such practice, but otherwise, should recognize the many types of network management practices that are reasonable. In addition, the convergence of different electronic communications in the IP Platform (voice, video, and text) and the massive growth of data transmission with these heterogeneous services, inherent in the

evolution of the internet service, has increased the need to use traffic management practices in order to assure that the users may access the information contents and services that they wish.

Any restriction to the use of reasonable traffic management practices can negatively affect the quality of the service and reduces the usefulness of the Internet for the users. There is a very high risk to the health of Internet networks, to expect that the operators have such concern with regulatory uncertainty that they refrain from carrying out investment and network management activity to render more efficient the network traffic or rate, to avoid running afoul of overly prescriptive regulatory measures. Instead, network operators must have the flexibility to employ reasonable network management that is beneficial to the user, and is required to be made, such as temporary storage of content, management of IP addresses for new users, blocking of a content because a parent wishes to prevent his children from having access to undesirable material.

Reasonable traffic management practices do not inherently degrade or impact other contents or applications that are less sensitive to transmission quality. The operation of the Internet network has been always based on algorithms that assure an adequate traffic handling and permit to assign each content the transmission capacity necessary as per its characteristics and specific critical nature. In order to make it possible, the internet operators have the potential to utilize IP transmission protocols that permit the identification of the different data packages that are transmitted over the network, so that the most critical ones or those requiring a greater transmission capacity may be reasonably prioritised over other types of traffic during the periods of greatest congestion in the network. Such reasonable network management practices can improve the traffic delivery experience for all service types, with the data accorded its appropriate priority (e.g. real-time two-way video requires a higher priority than email, in order to ensure a quality end user experience).

In fact, more than three decades ago, the Internet Engineering Task Force (IETF) established a command within the Internet Protocol in order to allow the prioritization of real time and other performance-sensitive applications[2]. The IETF broadened said capacity in years 1994 and 1998 through the creation of the "DSCP" or "DiffServ" field, and at present an even more advanced version of this capacity has been incorporated at IPv6. Traffic management in the form of package prioritization is made taking into account the performance of sensitiveness of the

[2]Information Sciences Institute, Internet Protocol DARPA Internet Program Protocol Specification, RFC 791, at 11 (Sept. 1981). Available at:http://www.ietf.org/rfc/rfc0791.txt.

applications. Thus, for instance, if a game application or an emergency IP call has a millisecond delay, the service experience of the user would be fully impacted and the use of the same would be discouraged. On the other hand, there are other contents or applications a little less sensitive to transmission rate, such as, for instance, the search for contents in the network or electronic mail consultation. The network prioritization practices, allows operators to selectively dedicate a greater bandwidth to the usage of the network that requires a greater transmission capacity, as distinct from the usage that tolerates certain degree of delay (latency) without impacting the user experience.

As recommended by the Organization for Economic Co-operation and Development (OECD)[3], the imposition of a new regulation based on speculations about possible future threats or damages is harmful to the markets and the users; specially in the case of a service as the Internet service that is in continuous evolution and needs to be fostered in order for the penetration of the same to be open to everyone. The OECD warned that the involvement of the new regulation in the traffic management activities and the requirement by the same of a neutral treatment of content packages would be premature[4].

ACTO shares this view and considers that the role of the regulators is to monitor the market and identify if real competition problems are arising and apply corrective measures specific to each case that are necessary and proportionate, leaving to the Internet Service Provider ("ISP") the management of every increasing volumes of IP traffic. According to the foregoing, instead of adopting restrictive regulations based on speculations that a market failure *could* eventually occur in the future, the regulator could issue general principles that ensure the essence of the Open Internet and if an operator is proven to deviate from such principles, the regulator has all the tools and powers to correct such conduct and reestablish the competition conditions of the market.

This light touch regulatory principle is all the more critical to meet the incredible projected demand for mobile broadband. While all broadband networks share the need for traffic management, given the ever rising demand for and proliferation of new quality-sensitive, bandwidth-intensive applications, mobile broadband networks also must contend with spectrum constraints, a shared "last mile" radio access network, interference sensitivity, and other

[3]Organization for Economic Co-operation and Development (OECD).Internet Traffic Prioritisation: An overview (2007 pg. 5). Available at:http://www.oecd.org/dataoecd/43/63/38405781.pdf.
[4]Ibid. Pg. 5.

concerns that make it far more challenging to provide mobile broadband than even fixed wireline broadband. Capacity and quality-of-service challenges for wireless broadband providers are particularly acute in the "last mile" radio access network, where spectrum is shared among both users and cell sites; bandwidth can fluctuate based on weather, interference and other issues; the number of users located in particular cells and their dispersion within those cells at any given time is variable; and the spectrum available for use is not infinitely (or even readily) expandable.

While it is impossible to predict which business models and engineering solutions will best meet consumers' diverse needs in this environment, subjecting the mobile industry to restrictions on network management would preclude many service-enhancing business arrangements and practices altogether, undermine efforts to manage scarce spectrum resources, chill sensitive engineering and business decisions through endless regulatory second-guessing or pre-emptive fear of enforcement, and deter investment and innovation in new network technologies.

In India, where a reported 97.5% of the more than billion connections to the internet by wireless subscribers[5], carriers must have the flexibility to use a range of dynamic network-management techniques to respond to or avert network failures or severe congestion and to ensure that customers can enjoy latency sensitive applications, such as voice calling and video streaming. As noted by the TRAI in the Consultation Paper No. 8/2015 on Differential Pricing for Data Services (9 December 2015), about 25% of the total wireless subscribers use wireless data (Internet) services in India. As of 30 June 2015, of the 300 million wireless Internet subscribers in the country, about 207 million subscribers used 2G (GPRS, EDGE and CDMA-1X) networks to access Internet, about 92 million subscribers use 3G (HSPA, WCDMA, EVDO etc.) and the rest used 4G LTE.

Mobile broadband service operators need to implement network traffic techniques to prevent or respond to network failures and handle congestion events in a fast and effective manner, thus preventing the service from being degraded and the user experience from being impacted. More invasive regulation of commercial and operational practices would cause significant difficulties if it was applied to mobile broadband, which comprises the large majority of Internet access services in many countries, including India.

[5] TRAI Pre-Consultation on Net Neutrality, 30th May, 2016, para. 1.

Q.3. What should be India's policy and/or regulatory approach in dealing with issues relating to net neutrality? Please comment with justifications.

ACTO's Response:

As the TRAI moves forward, we encourage moving towards a policy framework that will minimize regulatory burdens and provide the certainty that will promote the on-going, robust investment, competition and innovation. We encourage the Authority to apply any such regulation with the lightest possible touch that is competitively and technologically-neutral and avoid duplicative and inconsistent regulation to the benefit of consumers, competition and innovation and recognizes the benefits of excluding enterprise and specialized services from the regulatory construct. As noted above, to the extent that any regulatory intervention is found to be necessary to protect the Open Internet, it can be effective if appropriately targeted and limited to the adoption of meaningful transparency requirements, and the prohibition of blocking, degrading or otherwise unreasonably disfavoring some Internet traffic over other Internet traffic. However, there should be no restriction on user-driven prioritization, which can enhance social & consumer welfare and should be permissible.

Benefits of Light Touch Regulation

The TRAI should focus on adopting collaborative, self-regulatory initiatives among industry stakeholders. Where the market is effectively addressing public policy priorities, both consumers and competition benefit by reducing legacy regulation of communications services.

a) Flexible Rules are required to Foster Investment and Innovation

Competition in the mobile broadband marketplace is driving investment and innovation. Internet of Things ("IoT"), even in its still-nascent stage, has established itself as a growth engine throughout the global economy. IoT's importance will only continue to expand. IoT is revolutionizing entire industries by allowing Internet-connected machines to communicate directly with other Internet-connected machines, and with cloud computing platforms that analyze data coming off the connected devices, display it across user interfaces, and even provide input and direction back to the connected devices. These machine-to-machine (M2M) communications and the associated analytics platforms, all constituent parts of the IoT, have already demonstrated the potential to greatly improve efficiency, productivity, and social welfare in fields as diverse as education, healthcare, transportation, energy, security and agriculture. IoT technology is finding its way into almost every portion of our daily lives and our nation's economy: smart cities; connected cars; connected homes; remote telematics for almost

anything with an engine; fleet management; cargo tracking; personal wearable devices for health and fitness and for medical uses; and drones, just to name a few. The applications and technologies are complex and diverse, and the potential for new IoT applications seems almost limitless. Also, there is a contrast between mission critical IOT communications and communication which are not mission critical. It becomes essential that any regulations should not prevent the network provider from appropriately managing the network to differentiate between these different types of IoT applications. Like the app economy that sprouted in response to smart phones over the past decade, IoT presents immense opportunity for entrepreneurs and small businesses. With nearly ubiquitous wireless connectivity, Application Programming Interfaces (APIs) and off-the-shelf radio modules and other electronic components, inventors have already been developing a host of innovative new devices, applications, and solutions that will bring new levels of efficiency and productivity to many different segments of our lives and the economy.

A variety of novel business models, likely giving edge providers the option to trial the applications with pricing options that include Free Data will be a key component to many of the new applications and services that will characterize IoT in the future. By any measure, Free Data Platforms benefit content providers and consumers in the same way that toll-free calling and free shipping have provided comparable consumer and industry benefits for decades. These developments encourage innovation and consumer choice, and do not constitute an undue or unreasonable preference, a disadvantage, or unjust discrimination and will help support the growth of IoT.

b) Enterprise &Specialised Services Should Continue to be Exempt from Any Open Internet Rules

The TRAI should continue to exempt enterprise services from any Open Internet rules. Enterprise services, also sometimes called specialised services or business services, are typically offered to larger organizations through customized or individually negotiated arrangements. An example of such a service would be virtual private networks. Various jurisdictions that have reviewed open Internet policies have proposed to exempt such enterprise or specialized services from open Internet rules. In the United States, for example, both the *FCC's 2010 Open Internet*rules and the additional regulation adopted by the FCC in 2015 apply only to mass-market retail broadband Internet access service, with the capability to transmit and

receive data from all or substantially all Internet end-points.[6]This definition for the scope of the Open Internet rules excludes enterprise service offerings and specialised services such as virtual private networks.[7]

Other regulators have also avoided imposing net neutrality regulation on these enterprise or specialized services. Telecommunications and Internet providers throughout the world have long provided IP-based services to enterprise business customers. These services include enterprise-grade Internet access and Internet Protocol services, with the capability to prioritize packets associated with performance-sensitive applications. This is provided to a wide range of customers, including healthcare providers, community service organizations, restaurant chains, car dealers, electric utilities, banks, municipalities, security/alarm companies, hotels, labor unions, charities, and video-relay service providers. And the market of services that merit different network performance requirements is expanding with Smart Grid, healthcare, emergency-response, and a variety of other services that may involve or require packet prioritization capabilities. These services are pro-consumer, and indispensable to key social objectives. Just as other jurisdictions have recognized the merit for keeping these services outside the scope of open Internet rules, India also should not prescriptively regulate these services.

Q.4. What precautions must be taken with respect to the activities of TSPs and content providers to ensure that national security interests are preserved? Please comment with justification.

ACTO's Response:

The TRAI must balance the interests of national security and commerce. In framing any policy, the critical missions and legitimate needs of law enforcement agencies in their fight against terrorism and crime must be considered and we are committed to helping authorities in their efforts to seek reasonable and appropriate assistance from industry to protect public safety and national security to the extent permissible by the rule of law, including appropriate legal process and respect for the civil liberties and privacy rights of our customers. At the same time, we believe that government and law enforcement should respond to these technological changes

[6]*See* FCC, *Protecting and Promotingthe Open Internet*, GN Docket No. 14-28, Report and OrderOnDemand, DeclaratoryRuling and Order, rel.March 12, 2015 ("*FCC 2015 Internet Order*"), ¶¶ 186-187; FCC, *Preservingthe Open Internet*, 25 FCC. Rcd. 17905, ¶ 44 (2010)("*FCC 2010 Internet Order*").
[7]*SeeFCC 2015 Internet Order*, ¶ 190; *FCC 2010 Internet Order*, ¶ 47.

through fair, uniform procedures that govern when and how the government may compel any private company to provide access to customer information. Various government and law enforcement officials in India and worldwide should be discouraged from seeking ad hoc access to communication and security technologies to facilitate surveillance and interception operations beyond that which is permitted under the law.

We are firmly convinced that the integrity of all such technologies is indispensable to protect the safety and security of governments, citizens, businesses and civil society in India, as well as everywhere else. Smartphones and other personal devices contain a digital record of nearly every aspect of users lives that such users reasonably expect to remain within their personal control. Businesses likewise utilize encryption technology to help protect sensitive information belonging to the business and its customers which they too reasonably expect to remain within the control of the business. At the same time, the government is entitled to seek reasonable assistance from industry as necessary to protect public safety and national security. We recognize the need for legal regimes that respond to these technological changes through fair, uniform procedures that respect civil liberties and strike a fair balance between privacy and law enforcement, accounts for current technology, applies equally to all holders of personal information, and sets clear and appropriate limits on what government officials may compel companies to do.

However, these interests must be balanced against the need for companies – including service providers, content providers and OTT providers – and consumers to move data as they see fit. Many countries have enacted rules that put a chokehold on the free flow of information, which stifles competition and innovation. Thus, the TRAI should avoid erecting discriminatory and protectionist barriers and consider specific provisions designed to protect the movement of data, subject to reasonable safeguards like the protection of consumer data when exported. The TRAI should likewise consider that to support the Digital Economy in India, companies should not need to build physical infrastructure and expensive data centers in every country they seek to serve as such forced localisation requirements which add unnecessary costs and burdens on providers and customers alike. The TRAI should confront these localisation barriers through specific provisions designed to promote access to networks and efficient data processing.

Q.5 What precautions must be taken with respect to the activities of TSPs and content providers to maintain customer privacy? Please comment with justification.

ACTO's Response:

Consumers rightly expect their information will be highly secure and TSPs and edge provides will be respectful of their privacy. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Establishing this trusted environment for consumers across the ecosystem is crucial to the success in the market, separate and apart from the policy frameworks for these issues. However, information should be protected based upon the sensitivity of the information and how the information is used—not the type of business keeping it.

To the extent India looks to adopt Privacy rules, any such regulation of privacy and technology in India - and around the world - should reflect current market realities and be technology neutral so that rules and protections address the data that is collected, rather than the company collecting it. A framework which only applies to "publicly available electronic communications services in public communications networks," such as the ePrivacy Directive in the EU, is based on an outdated understanding that telecommunications companies have comprehensive and unique access to users' online activity as operators of the last mile of the network connecting end users to the Internet.

On the contrary, as a recent study by Peter Swire explains, policy decisions about the regulation of privacy practices of Internet Service Providers (ISPs) should take into account that access to user data by these companies is neither comprehensive nor unique.[8] According to Professor Swire, "[c]hanging technology and market practices create effective barriers to ISPs' visibility into their users' Internet activities." These include the fact that users often connect to the Internet with multiple devices and from multiple locations, as well as the increasing use of encryption, Virtual Private Networks, and other third-party proxy services.[9]

The aforementioned study indicates that edge providers – including Over-the-Top ("OTT") service providers, Web browsers, and Operating System developers – are the clear market leaders in tracking consumers and monetizing consumer online data. Google and Facebook

[8]see Peter Swire et al., *Online Privacy and ISPs: ISP Access toConsumer Data isLimited and OftenLessthan Access byOthers*, February 29, 2016 at 3, **attached as annexure-II** (http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps)

[9]Swire et al., *Online Privacy and ISPs*at 23-4.

alone account for more than 54% of digital advertising revenues and 67% of the mobile advertising market. Telecommunications companies and ISPs lag behind in this area in part due to healthy competition in the marketplace, which allows customers to change their ISP and wireless subscriptions regularly. Moreover, 42 of the top 50 Web sites currently use encryption by default or on user log-in, and nearly 70% of global Internet traffic will be encrypted by the end of 2016.

The TSPs and content providers should adopt suitable measures to maintain customer privacy as the customer expects their information will be highly secure and TSPs and content providers will be respectful of their privacy. One of the important aspects of the customer privacy is the availability of strong encryption over the networks to protect the customer information. Therefore there is a need to frame a suitable policy which balances the interest and need of all stakeholders including Government.

In light of these developments, the best way to ensure the protection of consumer privacy is through a competitively and technology neutral framework governing the collection of data, rather than different sets of rules for different entities collecting information. In today's world, where technology innovations are occurring at lightning speeds, policy makers should heed the European Commission's call in the Digital Single Market Strategy to ensure that regulatory frameworks provide "a level playing field for market players and consistent application of the rules." The Communication on Online Platforms and the Digital Single Market similarly states that regulators should "[e]nsur[e] a level playing field for comparable digital services," subject "comparable digital services … to the same or similar rules, duly considering opportunities for reducing the scope and extent of existing regulation," and "simplify, modernize, and lighten existing regulation." These principles are also echoed in the recent Centre on Regulation in Europe ("CERRE") Study on Consumer Privacy which concludes: "Consistent, future-proof regulation requires a common approach to all industries, regulated and unregulated alike. Sector-specific privacy regulations are inadequate in a dynamic environment and should therefore be withdrawn."[10] The report concludes sector specific regulations, such as the European Privacy Directive, can no longer be justified in a world of converged and globally connected online services.[11] An inconsistent approach, where consumers the level of protection consumers are afforded varies significantly depending on which technology or type of service

[10] Centre onRegulation in Europe (CERRE) PolicyReport, January 25, 2016, http://www.cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf, pages 6 and 16.
[11] Id.

provider they choose undermines consumer trust as users cannot rely on uniform rules to consistently protect their personal data and privacy. This weakens confidence in the digital ecosystem and stops consumers from benefitting fully from the potential of the market.

Therefore, in order to protect the confidentiality of consumers' communications and to enhance consumer trust, consumers should receive the same level of protection regardless of technology or type of service provider. Historically, this approach was adopted in the U.S. where the privacy policy has historically struck an important balance that targets potentially harmful uses of consumer data, while not interfering with the many beneficial uses of data. This approach had long been championed by the White House, Congress and the Federal Trade Commission "(FTC"). For two decades, the FTC's privacy framework applied to all companies operating in the Internet ecosystem, including ISPs and edge providers. However, a significant consequence of the *2015 Open Internet Order* is that it shifts authority over broadband privacy from the FTC to the FCC. In the pending Broadband Privacy proceeding, the FCC is proposing onerous limitations on the use of online data that would apply only to broadband providers. Edge providers (Google, Facebook, etc.) will continue to have greater flexibility to use the same online data under the FTC's privacy framework. Except for the passage of the *2015 Open Internet Order*, nothing has changed to warrant the FCC imposing extremely burdensome privacy rules that apply only to ISPs, while all other online companies are free to continue using that same consumer data with far fewer restrictions.

The potential onerous and confusing regulatory paradigm has elicited numerous comments, perhaps the most significant of which are those filed by the professional staff of the FTC itself with the unanimous approval of the FTC's current commissioners. The FTC's comments are a bracing reminder that many of the NPRM's proposals reflect basic misconceptions of complex online-privacy issues and would subject consumers to confusing and conflicting privacy regimes. As the FTC notes (at 8), "the FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of [ISP] services that would not generally

apply to other services that collect and use significant amounts of consumer data." [12] The FTC concludes, with considerable understatement, that "[t]his outcome is not optimal."[13]

The FTC's longstanding approach, calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to protect consumers.14 Thus, the FTC supports using opt-in for the content of consumer communications regardless of whether the company is a first party, affiliate, or third party, meaning all online companies other than ISPs are free to use non-sensitive customer-specific information to engage in first-party marketing without any consent mechanism, even opt-out.[15] But the proposed rules would subject ISPs to the most restrictive notice-and-consent mechanism—opt-in—before using customer-specific information for most first-party marketing and all third-party marketing. And they would rigidly impose that mechanism even if the information is as non-sensitive as mere customer names and addresses, and even if the ISP does not share that non-sensitive information with any third parties. As the FTC observes, the proposed consent regime "does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer. ... Therefore, FTC staff recommends that the FCC consider the FTC's longstanding approach, which *calls for the level of choice to be tied to the sensitivity of data*[.]" [16]

As the TRAI moves forward, we encourage the TRAI to recognize the importance of establish a uniform Privacy policy framework applicable across industries in India determined by the nature of the data, with the lightest possible touch, that is competitively- and technologically-neutral and avoid duplicative and inconsistent regulation to the benefit of consumers, competition and innovation.

---

[12] *See*: Comments of the Staff of the Bureau of ConsumerProtection of the Federal TradeCommission In theMatter of ProtectingthePrivacy of Customers of Broadband and OtherTelecommunicationsServices, FCC Docket 16-39, May 27th 2016, page 8) (FTC Comments) (https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf)

[13] *Id.*

[14] Id. at pg. 22 noting "Thisapproachisalsoconsistentwithexistinginternationalframeworks, such as the OECD PrivacyGuidelines, whichdistinguishbetweensensitive and non-sensitiveinformation.*See., e.g.*, OECD Privacy Framework at 16 ¶¶ 15(a)(ii), 18 (2013), *available at* http://www.oecd.org/sti/ieconomy/oecdprivacyframework.pdf."

[15] *Id. at pg. 20.*

Q.6. What further issues should be considered for a comprehensive policy framework for defining the relationship between TSPs and OTT content providers?

ACTO's Response:

Consistent with these overall objectives of Net Neutrality, there should be regulatory neutrality, such that the same services offer the same consumer protection whether offered by an OTT communication player or a TSP. Several OTT communication players have acquired significant dominance in the India market – for example WhatsApp now has 70 million users in India.[17] Similarly VoIP services like Skype and Viber have emerged as alternatives to traditional voice services. With the increase in competition between traditional and OTT communication services comes a legitimate need to frame policies based on the principle of apply "same policies to same services", based on the approach that best protects consumer interests.

Conclusion:

The TRAI should create a regulatory environment in India that will protect the Open Internet while preserving the incentives for investment and innovation that have propelled the necessary investment to support the remarkable and sustained growth of the "virtuous circle" that promotes innovation throughout the Internet ecosystem. To the extent that any regulatory intervention is found to be necessary to protect the Open Internet, it can be effective if it is appropriately targeted and limited to the adoption of meaningful transparency requirements, and the prohibition of blocking, degrading or otherwise unreasonably disfavoring some Internet traffic over other Internet traffic; does not restrict user-driven prioritization, does not apply to enterprise and specialized services; and is competitively- and technologically-neutral and avoids duplicative and inconsistent regulation. These principles are all the more critical for mobile networks given the unique constraints facing mobile broadband providers where the explosion in mobile broadband usage described above has required providers to develop innovative approaches to network management that must evolve quickly to provide the high-quality broadband experience that customers have come to expect.

If any additional regulation is required it should be based on evidence and ideally implemented in the form of principles which are applied ex-post and no ex-ante, to avoid prematurely dampening the highly dynamic and innovative nature of internet based services.

[17] https://techcrunch.com/2015/04/21/not-hatin-just-sayin/

We believe the TRAI can preserve Internet freedom and openness, and that it can do so without over-regulation so as to enhance broadband investment and deployment. The Internet has become the most powerful communications medium and engine for economic growth ever, and has achieved this unprecedented growth without prescriptive regulation of the Internet that would have locked in place certain specific technologies or business models. The TRAI should reject calls to ramp up regulation of ISPs and mobile broadband providers and recognize the remarkable state of competition, investment, and innovation among broadband providers that require permitting network operators the flexibility to manage their networks to the overall benefit of Indian consumers and to support the Government's objective of a Digital India.