# Reliance Communications Limited's Response to the Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks

## Executive Summary

A. **Adoption of e-KYC should be fast tracked for ease of authentication of subscribers over the WiFi Networks.**

B. **WiFi equipment that is compliant with standards such as IEEE's 802.11u or WiFi Alliance's Hotspot 2.0 or Wireless Broadband Alliance's Next generation hotspot should be mandated as it shall support seamless, automated authentication of the customers.**

C. **Promulgation of uniform RoW guidelines would go a long way in promoting public WiFi services.**

D. **The urban development ministry should include mandatory building of ducts, along the roads, for extending backhaul links and power lines to the WiFi equipment deployed on the street furniture.**

E. **Promulgation of uniform levies for utilization of street furniture for deployment of WiFi equipment shall facilitate proliferation of public WiFi services.**

F. **Promulgation of mandatory sharing of IBS / WiFi solutions deployed within a building shall provide the impetus for proliferation of public WiFi services.**

G. **The WiFi service providers should be integrated as resellers of TSPs / ISPs bandwidth as that shall facilitate single point of billing for the customers.**

H. **Mandated deployment of WiFi equipment that is compliant with standards such as IEEE's 802.11u or WiFi Alliance's Hotspot 2.0 or Wireless Broadband Alliance's Next generation hotspot shall address the customers security concerns due to the inherent security built into these specifications.**

I. **Interoperability between WiFi networks can be achieved through establishment of WiFi hubs / exchange models at the domestic / global level and establishment of interconnections between the hubs.**

J. **Interconnections shall have to be established amongst the cellular operators for ensuring interoperability between WiFi networks and cellular networks.**

K. **Due to the international level of operations by the WiFi hubs, TRAI's regulations for deciding the ceiling price of packs for WiFi services or the interconnection issues / pricing or any QoS requirements would be difficult to enforce.**

L. **Access services being licensed in India, provisioning of WiFi services should be permitted only through the agreements with the licensed TSPs / ISPs instead of through unlicensed and unregulated WiFi hubs.**

M. **No more frequency bands should be recommended for de-licensing, apart from frequency bands that have already been recommended by TRAI to DoT. Before de-licensing any additional bands, optimal exploitation of the existing bands should be ensured to expedite the penetration of broadband using Wi-Fi technology.**

N. **Frictionless access to public Wi-Fi hotspots, for domestic users as well as foreign tourists can be provided through effective KYC through means like, adoption of e-KYC, mandated deployment of WiFi equipment that is compliant to international roaming and automated authentication, prior registration of customers who intend using non-SIM devices, prior authentication of the customers over secure channels or through an App or through the usage of Credit Cards.**

O. **It is most ideal for the WiFi service providers to integrate their billing systems with that of the TSPs.**

P. **Modes of payment that are through the TSP / ISP, i.e. deductions from the core balance or included in the monthly post paid bills of the TSP, offer the most secure and frictionless transactions.**

Q. **There is a need to subject the hub operator to the regulations and guidelines of telecom services, especially for UL with Internet Service Class 'A' Authorization and compliance to DoT's instructions for provisioning WiFi services. The hub can be controlled by a private party under authorisation from the government similar to the Mobile Clearing House (MCH) for facilitating Mobile Number Portability.**

R. **It is feasible to have an architecture wherein a common grid can be created through which any small entity can become a data service provider and able to share its available data to any consumer or user.**

S. **It is this the right time to allow such reselling of data to ensure affordable data tariff to public, ensure ubiquitous presence of Wi-Fi Network and allow innovation in the market.**

T. **Promotion of hosting of data of community interest at local level, would lead to escalation of cost of data to the consumers instead of the envisaged reduction, hence it should not be advocated.**

Our specific comments on the issues posed by the Authority are given in the subsequent paragraphs.

## Detailed Response

### Question 1. Are there any regulatory issues, licensing restrictions or other factors that are hampering the growth of public Wi-Fi services in the country?

### Question 2. What regulatory / licensing or policy measures are required to encourage the deployment of commercial models for ubiquitous city-wide Wi-Fi networks as well as expansion of Wi-Fi networks in remote or rural areas?

### Our Response

**Yes, regulatory, licensing and miscellaneous issues such as cumbersome KYC requirements, non availability of RoW guidelines at the national level, lack of availability of structured ducts for extending backhaul links and power, Lack of Guidelines for use of Street Furniture / Lighting Poles, lack of IBS guidelines, non availability of seamless billing and user's concern for over the air security of communications are hampering the growth of public WiFi services in the country.**

1. The overload on cellular networks, particularly when it comes to data, is something that most subscribers across the majority of networks have experienced at some point. This effect is multiplied in environments where a large number of people are gathered, such as malls, stadiums, conferences, etc and all are trying to access services at the same time. Though these situations provide a good business opportunity for the TSPs as well as the premises owners alike, for deployment of WiFi services, but it is the following regulatory, licensing and miscellaneous challenges that prevent them from doing so.

   a. **Cumbersome Know Your Customer (KYC) Requirements.** KYC of the end users of telecom services is a mandatory license condition for all the telecom and internet service provisioning licensees. Since the possibility of misuse of internet access through WiFi hot spots, especially for anti national activities, is possible through non SIM devices as well, DoT has stipulated stringent KYC requirements that mandate ensuring traceability of the end user of the WiFi based internet services.

   b. For deployment of WiFi hot spots, DoT vide its letter number 820-1/2008 – DS Pl II dated 23 Feb 2006 has instructed all Internet Service Providers (ISP) to follow the registration and security procedures laid down in these instructions. As per these instructions,

      i. WiFi hotspot deployed, even by the end user himself, is mandated to be registered with the ISP and the services are mandated to be provisioned through secured access only.

      ii. For the provisioning public WiFi services, obtaining of POI from the customer has been mandated in these instructions.

   c. Such instructions though necessary have proved to be an impediment for the proliferation of public WiFi services due to the following perspectives of the users and that of the WiFi service providers.

      i. From the user’s perspective, provisioning multiple POIs for accessing the services, even at reduced rates, that he can otherwise access through his regular mobile connectivity, is not enticing enough to motivate them for subscribing to the WiFi service.

      ii. From the service providers perspective the additional setup that is required to be created and maintained for collection, verification, record keeping and auditing of the KYC records is not a financially viable solution.

   d. Therefore, it is recommended that,

      i. **Adoption of e-KYC should be fast tracked for ease of authentication of subscribers over the WiFi Networks.**

      ii. **WiFi equipment that is compliant with standards such as IEEE’s 802.11u or WiFi Alliance’s Hotspot 2.0 or Wireless Broadband Alliance’s Next generation hotspot should be mandated as it shall support seamless, automated authentication of the customers.**

   e. **Inconsistent Right of Way (RoW).** Deployment of WiFi hotspot requires adequate mechanism for backhaul of the data connectivity from the hotspot location. The inconsistent RoW guidelines, exiting in various municipal and other local bodies jurisdictions, are a major impediment for proliferation of public WiFi services. Therefore,

**promulgation of uniform RoW guidelines would go a long way in promoting public WiFi services.**

f. **Lack of Availability of Structured Ducts for Extending Backhaul Links and Power.** RoW arbitrariness apart, the lack of availability of structured ducts for extending backhaul links and power to the WiFi hotspot equipment proves to be a major impediment for proliferation of public WiFi services. Therefore, it is recommended that **the urban development ministry should include mandatory building of ducts, along the roads, for extending backhaul links and power lines to the WiFi equipment deployed on the street furniture.**

g. **Lack of Guidelines for use of Street Furniture / Lighting Poles for Deployment of WiFi Hotspots. .** Similar to RoW challenges, deployment of WiFi hotspots is challenged due to the arbitrary deployment levies imposed by the local authorities for utilization of the street furniture, including the lighting poles, for installation of the WIFi equipment. Therefore, it is recommended that **promulgation of uniform levies for utilization of street furniture for deployment of WiFi equipment shall facilitate proliferation of public WiFi services.**

h. **Lack of In Building Solutions (IBS) guidelines.** The lack of regulation of IBS guidelines is an impediment for deployment of WiFi services as it results in building owners either getting into exclusive agreements with one or two TSPs / WiFi service provider or demanding exorbitant rents for deployment / sharing of the WiFi infrastructure. Therefore, **promulgation of mandatory sharing of IBS / WiFi solutions deployed within a building shall provide the impetus for proliferation of public WiFi services.**

i. **Non availability of seamless billing across operators.** Non availability of seamless billing systems, across the public WiFi setups and the ISPs is a major challenge that prevents proliferation of public WiFi services. Integration of the billing systems would be facilitated when **the WiFi service providers are integrated as resellers of TSPs / ISPs bandwidth as that shall enable single point of billing for the customers.** Else, the services of any independent Wifi services provider vis-a-vis those of a reseller of TSPs / ISPs bandwidth shall be less affordable.

j. **User’s Concerns for Over the Air Security of Communications.** Security of communications is a mojr concern of the users preventing them from utilization of WiFi services, despite its advantages of faster connectivity and increased affordability of data services. As recommended above, **mandated deployment of WiFi equipment that is compliant with standards such as IEEE’s 802.11u or WiFi Alliance’s Hotspot 2.0 or Wireless Broadband Alliance’s Next generation hotspot shall address the customers security concerns due to the inherent security built into these specifications.**

**Our Recommendations**

2. In view of the impediments highlighted above which Recommendations for regulatory / licensing or policy measures that are required to encourage the deployment of commercial models for ubiquitous city-wide Wi-Fi networks as well as expansion of Wi-Fi networks in remote or rural areas are as given below.

   a. **Adoption of e-KYC should be fast tracked for ease of authentication of subscribers over the WiFi Networks.**

b. **WiFi equipment that is compliant with standards such as IEEE's 802.11u or WiFi Alliance's Hotspot 2.0 or Wireless Broadband Alliance's Next generation hotspot should be mandated as it shall support seamless, automated authentication of the customers.**

c. **Promulgation of uniform RoW guidelines would go a long way in promoting public WiFi services.**

d. **The urban development ministry should include mandatory building of ducts, along the roads, for extending backhaul links and power lines to the WiFi equipment deployed on the street furniture.**

e. **Promulgation of uniform levies for utilization of street furniture for deployment of WiFi equipment shall facilitate proliferation of public WiFi services.**

f. **Promulgation of mandatory sharing of IBS / WiFi solutions deployed within a building shall provide the impetus for proliferation of public WiFi services.**

g. **The WiFi service providers should be integrated as resellers of TSPs / ISPs bandwidth as that shall facilitate single point of billing for the customers.**

h. **Mandated deployment of WiFi equipment that is compliant with standards such as IEEE's 802.11u or WiFi Alliance's Hotspot 2.0 or Wireless Broadband Alliance's Next generation hotspot shall address the customers security concerns due to the inherent security built into these specifications.**

**Question 3. What measures are required to encourage interoperability between the Wi-Fi networks of different service providers, both within the country and internationally?**

**Question 4. What measures are required to encourage interoperability between cellular and Wi-Fi networks?**

**Our Response**

**Interoperability between WiFi networks can be achieved through establishment of WiFi hubs / exchange models at the domestic / global level and establishment of interconnections between the hubs.**

**Interconnections shall have to be established amongst the cellular operators for ensuring interoperability between WiFi networks and cellular networks.**

1. Many network operators, venue owners, and enterprises are leveraging unlicensed Wi-Fi technologies to provision faster data connectivity at selected sites. The industry is excited about the new protocols that can be leveraged for enabling seamless and complimentary connectivity between the WiFi networks alone or between the cellular and WiFi networks. The main requirement for interoperability between any networks is the ability of the hotspot to be able to detect the presence of the user, followed by the identification and selection of the parent TSP / ISP network of the user and finally authentication of the user, as a legitimate customer, by his parent network. Apart from traceability of the customer, this ability of the hotspot to be able to detect, Select and Authenticate the subscriber is necessary for billing purposes as well.

2. **Interoperability between WiFi to WiFi Networks.** As brought out in the CP itself, interoperability between multiple WiFi networks necessitates the establishment of a hub

wherein the WiFi networks connect to it as its spokes. These hubs can be established at the domestic / international levels by establishing one to one contracts with each of the WiFi hotspot hosting premise owner. Though such hubs have the ability to provide services at the WiFi Hubs internationally, however utilization of their services mandates procurement of the hub's service packs. Additionally, it is necessary for multiple hub operators to establish interconnections amongst each other to ensure interoperability of the each other's WiFi hotspots. It is brought out that **due to the international level of operations, TRAI's regulations for deciding the ceiling price of packs for WiFi services or the interconnection issues / pricing or any QoS requirements would be difficult to enforce.**

3. **Interoperability between WiFi Networks and Cellular Networks.** WiFi is just another mechanism for provisioning access to the services of the cellular network. Therefore, WiFi hot spots are inherently interoperable with the backhaul cellular networks. However, interoperability of WiFi hotspots of different cellular networks would entail establishment of interconnections and conclusion of interconnection agreements amongst the cellular operators, once again for the purpose of detection, selection, authentication and subsequently billing.
4. However, it is brought out that provisioning of access service through WiFi is similar to any other form of access service and needs to be regulated as per the regulations and guidelines established under the Indian Telegraph act, 1885. Therefore, it is recommended that **provisioning of WiFi services should be permitted only through the agreements with the TSPs / ISPs instead of through WiFi hubs.**

## Our Recommendations

5. **Due to the international level of operations by the WiFi hubs, TRAI's regulations for deciding the ceiling price of packs for WiFi services or the interconnection issues / pricing or any QoS requirements would be difficult to enforce.**
6. **Access services being licensed in India, provisioning of WiFi services should be permitted only through the agreements with the licensed TSPs / ISPs instead of through unlicensed and unregulated WiFi hubs.**

**Question 5. Apart from frequency bands already recommended by TRAI to DoT, are there additional bands which need to be de-licensed in order to expedite the penetration of broadband using Wi-Fi technology? Please provide international examples, if any, in support of your answer.**

## Our Response and Recommendations

**No more frequency bands should be recommended for de-licensing, apart from frequency bands that have already been recommended by TRAI to DoT. Before de-licensing any additional bands, optimal exploitation of the existing bands should be ensured to expedite the penetration of broadband using Wi-Fi technology.**

**Question 6. Are there any challenges being faced in the login / authentication procedure for access to Wi-Fi hotspots? In what ways can the process be simplified to provide frictionless access to public Wi-Fi hotspots, for domestic users as well as foreign tourists?**

**Our Response**

1. Given the volatile political situation in our country, it is important for the law enforcing agencies to be able to keep a tab and trace individuals who indulge in anti social and anti national activities. Accordingly, KYC of the end user of telecom service has been mandated in the license conditions for the access services authorisation.

2. As brought out in our response to question number 1, for deployment of WiFi hot spots, DoT vide its letter number 820-1/2008 – DS PI II dated 23 Feb 2006 has instructed all Internet Service Providers (ISP) to follow the registration and security procedures (POI of the end user) laid down in these instructions. **The challenges that are faced while implementing these instructions are as given below**,

   a. **Collection of POI at the hotspot location.**

      i. A customer is exposed to multiple WiFi networks in public places such Malls, Heritage places, etc. From the user's perspective, provisioning POIs repetitively for each and every location is a cumbersome process, which the customers prefer to avoid.

      ii. Additionally, the WiFi service provider has to rely on the honesty of the individual providing the POI, as there are no means for immediate verification of the authenticity of the POI by the WiFi service provider. This problem gets accentuated further for the foreign nationals.

      iii. It is equally challenging for the WiFi service provider to establish an additional setup for collection, verification, record keeping and auditing of these POI records.

   b. **Delivery of OTP at the Hotspot site.** To overcome the challenges of collection of POI at the hotspot site, TSPs have started providing OTP on the registered mobile numbers of the subscriber. However, pitfalls of this system are that it mandates that

      i. Necessary to have a SIM Enabled Device. The subscriber should necessarily have a SIM enabled device / another device which can receive an OTP message for a non SIM enabled device.

      ii. Lack of Availability of Mobile Coverage. There should be mobile coverage at the place of usage of WiFi services for receiving the OTP. E.g. Though WiFi services are available at the New Delhi's Airport Express metro stations; however, the biased IBS services have ensured that mobile signals of most of the TSPs are not available at the underground metro stations, thereby denying the opportunity of usage of the WiFi services by the customers.

      iii. International Roaming Charges for the Foreign Nationals. The problem gets even more challenging for the foreign tourists who are required to pay international roaming charges for receiving the OTP thereby negating the advantages of cheaper WiFi services.

**Our Recommendations**

3. **The ways in which these processes can be simplified to provide frictionless access to public Wi-Fi hotspots, for domestic users as well as foreign tourists are as given below**,

a. **Adoption of e-KYC.** Adoption of e-KYC should be fast tracked for ease of authentication of subscribers over the WiFi Networks.

b. **Mandated deployment of WiFi equipment that is compliant to international roaming and automated authentication standards.** WiFi equipment that is compliant with standards such as IEEE's 802.11u or WiFi Alliance's Hotspot 2.0 or Wireless Broadband Alliance's Next generation hotspot should be mandated as it shall support seamless, automated authentication of the customers.

c. **Usage of Credit Cards for Authentication.** Individuals who can pay for the WiFi access using a credit card should be authenticated based on the credit card usage itself. This shall facilitate the usage of WiFi services by the foreign customers.

d. **e-CAF / Online CAF (As suggested in the CP at para 3.14 (c)).** Though a highly practical idea, it is brought out that this methodology would require amendment of the license conditions. In case DoT is amenable to the idea of e-CAF and its digital authentication by leveraging Aadhar information, the TSPs would be more than willing to accept the same.

e. **Prior Registration of Customers who Intend Using Non-SIM Devices.** As stated above provisioning OTP to the non SIM devices is a challenge. Hence, the above suggested modes of e-payment too would not suffice for Identification and authentication of an individual. It is therefore recommended that use of any WiFi only devices should be mandated to be registered in advance, with any TSP who has done the KYC of that customer.

f. **Prior Authentication of the Customers, Over Secure Channels, Through an App.** TSPs can facilitate availability of an App / Website for their customers, through which the customers can authenticate themselves using 'User name' and 'Password'. The operators can store the User's device Mac ID & the registered mobile number (on which the OTP was sent at the time of registration) for identification of the customer, every time the customer's device is within the coverage of a WiFi hotspot. Apart from making the access frictionless, this can even facilitate availing of services by the foreign nationals.

**Question 7. Are there any challenges being faced in making payments for access to Wi-Fi hotspots? Please elaborate and suggest a payment arrangement which will offer frictionless and secured payment for the access of Wi-Fi services.**

**Question 9. Is there a need for ISPs/ the proposed hub operator to adopt the Unified Payment Interface (UPI) or other similar payment platforms for easy subscription of Wi-Fi access? Who should own and control such payment platforms? Please give full details in support of your answer.**

**Our Response**

**No challenges are being faced in making payments for access to Wi-Fi hotspots.**

**Yes, adoption of the Unified Payment Interface (UPI) or other similar payment platforms for easy subscription of Wi-Fi access, by the ISPs/ the proposed hub operator shall facilitate proliferation of WiFi services.**

1. WiFi service providers can be classified into the following types and the payment modes of each are described against each.

| Type of WiFi Service Provider | Source of Backhaul Bandwidth | Revenue Model Adopted | Payment Mode |
|---|---|---|---|
| Local WiFi service provider (Similar to the PCO kind described in the consultation paper) | Any TSP / ISP | 1. Pay as you go.<br>2. Time bound utilization package.<br>3. Data Volume based utilization package. | 1. Local across the counter.<br>2. Through Unified Payment Interface / payment portals like PayTM, etc. |
| Sponsored WiFi Service Provider | Any TSP / ISP | Free usage | NA |
| Hub type service provider | Many TSPs / ISPs | 1. Advertisement revenue.<br>2. Revenue sharing with the TSP / ISP.<br>3. Pay as you go.<br>4. Time bound utilization package.<br>5. Data Volume based utilization package. | 1. Can be permitted through the TSP's / ISP's core balance.<br>2. Included in the monthly post paid billing by the TSP / ISP.<br>3. As service vouchers purchased across the counter.<br>4. Through Unified Payment Interface / payment portals like PayTM, etc. |
| UL(VNO) with Internet Service Authorization | Single TSP / ISP | | |

2. From the table above it is observed that the modes of payment that are through the TSP / ISP, i.e. deductions from the core balance or included in the monthly post paid bills of the TSP, offer the most secure and frictionless transactions.

## Our Recommendations

3. **It is most ideal for the WiFi service providers to integrate their billing systems with that of the TSPs.**

4. **Modes of payment that are through the TSP / ISP, i.e. deductions from the core balance or included in the monthly post paid bills of the TSP, offer the most secure and frictionless transactions.**

**Question 8. Is there a need to adopt a hub-based model along the lines suggested by the WBA, where a central third party AAA (Authentication, Authorization and Accounting) hub will facilitate interconnection, authentication and payments? Who should own and control the hub? Should the hub operator be subject to any regulations to ensure service standards, data protection, etc?**

**Our Response and Recommendations**

1. **Yes, there is a need to adopt a hub-based model along the lines suggested by the WBA, where a central third party AAA (Authentication, Authorization and Accounting) hub will facilitate interconnection, authentication and payments.**
2. **The hub can be controlled by a private party under authorisation from the government similar to the Mobile Clearing House (MCH) for facilitating Mobile Number Portability.**
3. **Yes, there is a need to subject the hub operator to the regulations and guidelines of telecom services, especially for UL with Internet Service Class 'A' Authorization and compliance to DoT's instructions for provisioning WiFi services.**

**Question 10. Is it feasible to have an architecture wherein a common grid can be created through which any small entity can become a data service provider and able to share its available data to any consumer or user?**

**Question 11. What regulatory / licensing measures are required to develop such architecture? Is this a right time to allow such reselling of data to ensure affordable data tariff to public, ensure ubiquitous presence of Wi-Fi Network and allow innovation in the market?**

**Our Response and Recommendations**

**Yes, it is feasible to have an architecture wherein a common grid can be created through which any small entity can become a data service provider and able to share its available data to any consumer or user.** Networks like the Bharat Net / any TSP / ISP can be leveraged by any small entity / an individual to provision localised WiFi based internet access to the local population.

However, **the local WiFi service provider shall have to comply to the KYC requirements of the DoT before provisioning WiFi services.**

**Yes, it is this the right time to allow such reselling of data to ensure affordable data tariff to public, ensure ubiquitous presence of Wi-Fi Network and allow innovation in the market.** In May 2015, DoT has already introduced UL(VNO) with Internet Service Authorization and hence, an entity can be a reseller of the TSPs / ISPs bandwidth.

**Question 12. What measures are required to promote hosting of data of community interest at local level to reduce cost of data to the consumers?**

**Our Response**

1. It is felt that in this era of cloud computing, **promotion of hosting of data of community interest at local level, would lead to escalation of cost of data to the consumers instead of the envisaged reduction.** Cloud computing is characterised by cost savings through economy of scales and reversing the same would also result in reversing of the gains on cost savings on account of CAPEX and OPEX.

2. Hosting of data at the local level would require availability of highly skilled manpower that is able to handle tasks such as Server and Storage Administration, management of AMCs, Software license Management, Virtualization, Router, Switches, load balancer, synchronisation with the master servers once the links are restored, Environment control and power management systems, etc. At no point is it going to be limited to a single server setup as the services suggested to be provisioned (children's study materials, educational data, agricultural and health related information, as well as movies and entertainment content) in the CP will mandate establishment of a server farm.

3. Given the state of awareness and consequently the demand for digital services in the rural hinterland, it is felt that the teething requirement of availability of services without the backhaul being available is unlikely.

**Our Recommendations**

4. In view of the above, it is recommended that since **promotion of hosting of data of community interest at local level, would lead to escalation of cost of data to the consumers instead of the envisaged reduction, hence it should not be advocated.**