Wireless Broadband Alliance (WBA) response to Telecom Regulatory Authority of India (TRAI) Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks (Consultation Paper No. 14/2016)

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to champion the development of the converged wireless broadband ecosystem through seamless, secure and interoperable unlicensed wireless broadband services for delivering outstanding user experience. Building on our heritage of NGH and carrier Wi-Fi, WBA will continue to drive and support the adoption of Next Generation Wi-Fi services need coexistence and convergence of unlicensed and licensed networks across the entire public Wi-Fi ecosystem, including IoT, Big Data, Converged Services, Smart Cities, 5G, etc. Today, membership includes major fixed operators such as BT, Comcast and Charter Communications; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel. WBA member operators collectively serve more than 2 billion subscribers and operate more than 30 million hotspots globally.

Issues for Consultation

Q1. Are there any regulatory issues, licensing restrictions or other factors that are hampering the growth of public Wi-Fi services in the country?

I. *The current limited availability of 5 GHz spectrum and the fact that some of the 5 GHz sub-bands are not license-exempt for outdoor use, are significant barriers to achieving the outdoor Public Wi-Fi coverage that is needed to meet demand. These sub-bands can be effectively utilized for both public access for consumer devices and as well as used for shorter-range backhaul links where fiber or copper is not available, as often is the case. The fact that outdoor use in these sub-bands is not license-exempt also deters opportunistic and entrepreneurial deployments by service providers or property owners.*

II. *We recommend that TRAI to consider:*
    a. *allowing license-exempt outdoor use throughout the continuous range of 5150-5350 MHz.*
    b. *allowing license-exempt use of the 5470-5725 MHz band, which is utilized in many countries*
    c. *allowing license-exempt use of the 5725-5825 MHz band for higher power (4W EIRP) outdoor usage*
    d. *extending the 5 GHz band by allocating 6GHz for license exempt use*

III. *The Internet Service License security requirements for Public Wi-Fi have likely also limited deployments due to the need to deploy, administer, and maintain the infrastructure services to register, provision, and track users. However, as TRAI notes in its Consultation Paper, newer Wi-Fi technologies such as Passpoint can help reduce this burden by standardizing the mechanisms and allowing smaller operators or entities to focus on providing the Public Wi-Fi access networks, while partnering with other entities for the authentication and tracking of users.*

Q2. 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?

I. *The limited availability of facilities-based fiber or copper broadband services throughout the country, including within cities - but especially in suburban and rural areas, will continue to constrain availability of Public Wi-Fi. In recent years, significant technological advances and investments have been made in so-called "wireless broadband" solutions that will utilize the millimeter wave (mmWave) bands to deliver very high capacity service as a lower cost alternative to fiber. These solutions could be extremely effective in providing the backhaul connectivity from Public Wi-Fi deployments in the many locations where fiber or copper backhaul is not available.*

II. *We strongly support the Authority for its November 2015 recommendation that the V Band (57-64 GHz) should be delicensed for indoor and outdoor based access applications like Wi-Fi hotspots etc. We suggest that the Authority and Department of Telecommunications consider a very lightly licensed approach for backhaul applications, both point-to-point and point-to-multipoint, in the V Band. Such an approach could still require the WPC registration, but further reduce the license cost in order to open the backhaul applications, and thereby Public Wi-Fi deployments, to a broader group of participants.*

III. *We also recommend that the Authority to consider allowing license-exempt use, both access and backhaul, in the 64-71 GHz range with appropriate power limits. This would provide more resources for wireless backhaul services, especially in the urban environment where spectrum demand will be highest, and would also be consistent with the recent action of the US FCC, thereby benefiting from greater economies of scale.*

IV. *We request that TRAI should permit channel bandwidths in accordance with the IEEE 802.11ad standard at 2.16 GHz.*

Q3. What measures are required to encourage interoperability between the Wi-Fi networks of different service providers, both within the country and internationally?

I. *In terms of the radio access link, adherence to IEEE 802.11 specifications and certification under the appropriate Wi-Fi Alliance programs are the primary methods to ensure interoperability between Wi-Fi devices (infrastructure and clients) and from network to network.*

II. *Wi-Fi Alliance Passpoint program, launched in 2012, offers reliable and secure connection experience for users as well as Interoperability between the Wi-Fi networks of different wireless carriers.*

III. *From a regulatory perspective, harmonization of Wi-Fi bands and their rules for use with other major markets (to the extent possible) helps limit incompatibility issues, and also reduces cost and improves availability of (network) devices.*

IV. *Regarding the interconnections to allow transparent access between service providers, please see our responses to Questions 6 and 8.*

Q4. What measures are required to encourage interoperability between cellular and Wi-Fi networks?

There are two general sets of technology options to address cellular / Wi-Fi interoperability.

I. *The first set can be termed "Cellular / Wi-Fi Interconnect" and involves 802.1X secure Wi-Fi access with authentication of a mobile device credential (SIM or USIM) by a cellular operator. The Wi-Fi network can be owned/operated by the mobile operator, or by a partner/service provider that also is able to support 802.1X secure access.*
    a. *In the case of Passpoint, this type of access is further enhanced via an automatic discovery and selection capability which means the user no longer needs to take any steps to connect to the Public Wi-Fi network initially, but rather the device will connect whenever in range of a network supporting its credential.*
    b. *These 802.1X/Passpoint solutions are well-understood / mature and are in active deployment globally. We will discuss the measures that can be taken to support these types of deployments in our answers to Questions 6 and 8.*

II. *The second set of options can be termed "Cellular / Wi-Fi Integration". These include LTE-WLAN Aggregation (LWA) and LTE WLAN Integration with IPsec Tunnel (LWIP), which are both 3GPP Release 13 programs – meaning that they have just recently been specified, with commercial deployments expected in mid-2017. Unlike the interconnect solutions above, which continue to see the Wi-Fi and cellular networks as separate domains and simply facilitates secure Wi-Fi access using the cellular credential and core, these newer integration options actually allow a mobile LTE network operator to utilize Wi-Fi networks to increase the overall capacity of the LTE service to their subscribers. Similarly, to the interconnect solutions, the Wi-Fi network can be either owned/operated by the mobile operator or by a partner. Because these solutions are so new, there are no known regulatory implications at this time – but we anticipate that they will be similar to the ones we address in Questions 6 and 8 as the basis for partner based-integration.*

Q5. 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.

As mentioned in our responses to Questions 1 and 2, we recommend the following de-licensing arrangements:

Recommendation	***International Examples***
Allowing license-exempt outdoor use throughout the continuous range of 5150-5350 MHz	*The FCC eased the restrictions on the 5150-5250 MHz sub-band allowing outdoor use and higher transmit powers, and Ofcom is considering easing its rules to permit outdoor use in the 5150-5350 MHz sub-band.*

Allowing license-exempt use of the 5470-5725 Mhz band	*Following the decision of WRC-2003, many countries permit unlicensed RLAN use under the regulatory conditions in the Radio Regulations*
Allowing license-exempt use of the 5725-5850 MHz band for higher power (4W EIRP) outdoor usage	*5725 – 5850 MHz is widely used in the US by cable operators to deploy extensive Wi-Fi services in dense area's*
Allowing license-exempt use of the 6 GHz band as an extension to the 5GHz band	*The International Telecommunications Union (ITU) has conducted some sharing studies between IMT and FSS and FS. In 2013 Russia proposed in CEPT brief that 5925-6425 be considered as a candidate for mobile broadband.* *The WBA has made this request in its recent response to an Ofcom consultation*
mmWave Frequency Range • *Allowing license-exempt use, both access and backhaul, in the 57-64 GHz range. A channel bandwidth size of 2.16 GHz (not 50 MHz as stated in item 3.7 of the consultation paper) as standardized by IEEE Standard 802.11 ad-2012 and adopted globally is recommended.* • *Allowing license-exempt use, both access and backhaul, in the 64-71 GHz range with appropriate power limits; a channel bandwidth size of 2.16 GHz as being standardized by IEEE Project 802.11-REVmc.*	*US FCC (Report and Order and Further Notice – FCC-16-89A1) made additional adjacent spectrum available on a license-exempt basis and currently the entire 57-71 GHz frequency band is available for license-exempt outdoor use.*

Q6. 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?

I. *Previously, the complexity of accessing Wi-Fi Hotspots (selecting the correct SSID in the first place) and then authenticating (navigating a captive portal of some type and obtaining a valid credential) has severely impacted the adoption and use of Public Wi-Fi services. This is also reinforced by regulatory and consumer concerns about the privacy and security of Public Wi-Fi which is almost always traditionally delivered over an Open/Unsecured SSID (even when initially authenticated with a Captive Portal). Industry has responded to provide solutions to these concerns.*

II. *Network Authentication Solutions[1]:*

a. *To address the complexity and security concerns and to create seamless and secure access, the Wi-Fi Alliance Passpoint program and the Wireless Broadband Alliance Next Generation Hotspot Interoperability program were launched and successfully concluded.*

b. *Passpoint is generally supported by all major network equipment providers. Most carrier-grade or enterprise-grade legacy networks are capable of providing 802.1X (SIM/USIM or TTLS/TLS credentials) authentication.*

c. *On the client side, Passpoint Release 1 is now supported in leading mobile operating systems (Android and iOS) and also on major PC operating systems (Windows 10 and MacOS).*

d. *Deployments of Passpoint /NGH can currently be seen in 3 major groups:*

i. *cable and fixed-line network operators, Wi-Fi service providers, and mobile network operators*

ii. *large public venues such as airports, convention centers, and (downtown) urban centers. Municipalities have started to deploy Passpoint Public Access networks, such as the cities of New York, San Francisco, and San Jose. These networks allow citizens and guests to perform a one-time secure registration and apply for authentication credentials, after which they enjoy automatic and secure connectivity to the municipal Public Wi-Fi network. In some cases cities have also implemented roaming with other cities and/or operators.*

iii. *small retail (SMB) venues via operator-managed broadband and Wi-Fi service packages.*

III. *Compliance of regulatory requirements using Next Generation Hotspot (NGH)*

a. *User identification can be provided by NGH networks by using a SIM/USIM, or other securely provisioned and stored credentials (username/password or client certificate – TTLS/TLS). These identifiers apply to both domestic as well as foreign Passpoint users. The credentials can be used to trace back identity information as and when required.*

b. *Moreover, Passpoint newest release - starting to be trialed - will deliver mechanisms for online sign-up. The user will be able to select the provision method and operator on the spot, and use Wi-Fi from that point on in seamless and secure fashion, across the footprint of the operators, partner venue, and (foreign) roaming partners.*

c. *For countries with similar regulatory requirements as India, the WBA has carried out temporary deployments to match these requirements with Passpoint and NGH capabilities.*

[1] Public Access Wi-Fi mechanisms to address the complexity and security concerns was undertaken beginning in 2011 with the publication of the IEEE 802.11u specification, which was followed in 2012 with the Wi-Fi Alliance Hotspot 2.0 technical program, and the Wireless Broadband Alliance Next Generation Hotspot interoperability program. The Wi-Fi Alliance Passpoint certification is based on the Wi-Fi Alliance Hotspot 2.0 Specification

NGH/HS2.0 Aiding APAC Regulators/Operators

Context

Example of APAC Countries with strict Wi-Fi access regulation who have implemented HS2.0/NGH

Indonesia

Thailand

Regulatory Requirement	NGH/HS2.0 Enhancements
All users must complete a registration with personal information before being allowed to connect to a Wi-Fi network	Information of the user automatically sent to the partner network via SIM card or credential in advance provisioned in the device
Must use a captive portal to follow this process, subject to congestions, security and privacy concerns and cyber attacks	Connection is seamless, device automatically searches and connects to partner networks without user intervention
Most partner networks only allow SIM-based authentication by receiving a SMS (e.g. one-time password), leaving out all the remaining non-mobile users	Supports both the mobile users (via SIM authentication), Wi-Fi only or other users by using credential stored on the phone or device
Foreign access is troublesome as users from some countries are not supported nor have possibility of making a connection	Seamless roaming is allowed; leveraging on interconnection with other international partner networks enables virtually every user to connect

IV. *Consumer benefits*

a. *When utilizing the same 802.11u / Passpoint mechanisms, roaming and interconnect relationships can be formed with other partner networks (cities, network operator, and other service providers, etc.) to alleviate the requirement for different authentication methods for different Wi-Fi hotspots.*

b. *Operators are able to use roaming relationships with one another, whereby the subscribers of one operator are able to automatically and securely connect to the Wi-Fi footprint of a partner utilizing the 802.11u and Passpoint mechanisms, with the backend authentication and accounting interconnection being done in conformance with the Next Generation Hotspot program. Some examples of operator-to-operator Wi-Fi roaming include Boingo and Time Warner Cable (Charter Communications), Boingo and Sprint, , and Liberty Global Inc. and Comcast. Obviously, also existing roaming relationships with mobile operators can be leveraged.*

V. *The existing regulatory requirements governing public Wi-Fi networks are overly prescriptive and adversely impact user experience and convenience. Such requirements discourage users from signing on to public Wi-Fi services. Rather than laying down prescriptive security requirements including Know Your Customer (KYC) compliance, the government should define the security requirements at a high level and allow industry the flexibility to deploy mechanisms to meet those requirements. The policy should emphasize outcomes and not on the process for achieving the outcomes. With modern technologies (for example that allow SIM based identification), Wi-Fi providers should be able to address government's security concerns in a way that would not hinder user experience. The adoption of such*

technologies and adherence to industry standards allow Wi-Fi service providers to provide seamless user authentication across networks. The hub model, on the other hand, can enable central authentication across participating Wi-Fi networks.

Q7. 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.

I. *Passpoint authentication is based on an existing (commercial and non-commercial) relationship between a subscriber and an entity (e.g. mobile network operator, service provider, venue or city) and use the operator's billing mechanism to settle payments with the subscriber, both for pre-paid and post-paid subscriptions. Equally, in operator-to-operator roaming scenario's, both billing and financial settlement are handled through commercial roaming agreements. In city/venue roaming scenario's, the parties might agree only to provide authentication without financial settlement in cases where free Wi-Fi access is provided.*

II. *Payment issue is not specific to public Wi-Fi but needs to be addressed from the larger perspective of digital economy. Free market dynamics should be allowed to come out with various solutions. Government should not mandate any specific platform(s), rather it should support emergence of multiple payment solutions through appropriate policy interventions.*

Q8. 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?

I. *While not architecturally mandatory since direct peer-to-peer interconnects can be implemented, in order to achieve the maximum coverage with and participation in an interconnected country-wide Public Wi-Fi network multiple centralized roaming hub services would be critical.*

II. *Such services allow very easy interconnect, by forming large spokes of interconnectivity amongst various network operators and then forming even larger webs of interconnectivity by peering with other roaming hubs. When a new operator joins the 'web' by connecting to any one of the hubs, they are then able to interconnect with any other operator on the 'web' via a contractual/business arrangement. This also includes mobile to Wi-Fi interconnects as mentioned in Q4.*

The WBA has demonstrated several times the applicability and benefits of such an approach during the NGH Live demonstrations at WBA Wireless Global Congress and Mobile World Congress where mobile operators, non-mobile operators, service providers, venues and cities provided free roaming during these events.

III. *The parallels to the development of the overall public Internet are obvious in terms of reach, economies of scale, and exponential growth. This type of hub-based*

approach also makes it easier to smaller operators or even private entities to partner with larger operators while direct peering might never be feasible.

IV. *Already several private entities with the business experience, technical competency, security and financial stability can ensure interconnect services will be reliably available for a pre-determined duration.*

V. *The WBA Wireless Roaming Intermediary eXchange (WRIX) framework defines the standards around interconnectivity between operators and the roaming hub services, see below picture with WRIX building blocks. The WBA Interoperability Compliance Programme can ensure that the interoperability requirements for roaming are being met to the required criteria.*

Q9. 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.

I. *Using Passpoint and NGH (as addressed in Q8) alleviates the requirement for creating a Unified Payment Interface for those users that already are a (pre- or post-paid) subscriber of an operator/service provider as payments will be settled via commercial roaming agreements.*

II. *For other instances, a Unified Payment Interface or common payment platform might be considered as part of the captive portal, as long as the security of the payment interface can be guaranteed, similar to the secure payment gateways that are provided by banks and credit card companies.*

Q10. 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?

The abovementioned roaming architecture, where operators/service providers utilize to roaming hubs to facilitate interconnect services at an international level, could also be implemented at a national level and as such can also facilitate roaming between domestic data service providers and create the proposed "common grid". There could be multiple grid providers. The government should not create a monopoly but instead allow entry of multiple players.

The "common grid" should adhere to a standardized framework, such as the WBA Wireless Roaming Intermediary eXchange (WRIX) framework. Such framework will define the common interconnect requirements of data service providers to roaming hub as well as the common interconnect requirements between roaming hubs. It will also provide guidance on the type of supported authentication methods.

Q11. 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?

The abovementioned WRiX framework provides data service providers and roaming hubs with the necessary requirements to create interconnections between data service providers and roaming hubs. The WRiX framework also provides documentation that is required for the exchange of information for billing, data clearing and reporting.

The WRiX framework could be used to ensure that an open architecture is used between domestic service providers to share data.

However, the WRiX framework assumes that the parties have agreed in advance on the commercial terms of the roaming agreement, so that these terms can be implemented into the billing and rating information.

The market forces should be allowed to mature the ecosystem without any regulatory intervention. No prescriptions should be made on standards and technologies but the ecosystem should be allowed to evolve.

Q12. What measures are required to promote hosting of data of community interest at local level to reduce cost of data to the consumers?

No Comment.

Q13. Any other issue related to the matter of Consultation.

We respectfully suggest that the Authority revisit the definition of "Broadband" services with a criterion of only 512 Kbps download speed. The continuing growth of video

*consumption in both private and public settings will require multiple Mbps downlink speeds. Additionally, the proliferation of social media, resultant content sharing, and cloud-based storage/synchronization from mobile devices is creating more uplink traffic, with some high-density Public Wi-Fi venues such as stadiums and arenas seeing about a 50/50 mix of uplink and downlink traffic. We would recommend a definition of not less than 2 Mbps bidirectiona*l.

Any enquiry to WBA regarding this document should be sent by e-mail to the care of Ton Brand (ton@wballiance.com) or Tiago Rodrigues (tiago@wballiance.com) or by letter to:

Wireless Broadband Alliance Ltd
8 Eu Tong Sen Street #14-94
The Central, Singapore 059818