Comments to the Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks

Introduction

In India, as per the subscription data[1] released by TRAI wireless subscriptions constitute 88 % of broadband connections. Thus, the Internet revolution in India is largely fueled by mobile devices. Hence, to ensure proliferation of broadband, optimum use of wireless technologies, especially Wi-Fi is essential.

Although Wi-Fi networks are affordable and scalable, there are technical and legal obstacles that have to be surmounted to ensure effective adoption of this technology as a means for bridging the digital divide. Legal and policy challenges in this context include ambiguity around the law governing Wi-Fi networks and de-licensing of spectrum.

With the roll-out of National Optical Fibre Network, almost all Panchayats will have high-speed optical fibre connectivity. However, the last mile and the middle mile issues will still remain. This problem could be solved by utilising TV White Spaces for the middle mile and adoption of Wi-Fi technologies for the last mile. This could also spur local innovation and entrepreneurship with management of Wi-Fi hotspots and connectivity solutions.

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?

There exists an extent of ambiguity as regards the legal and policy governance of public Wi-Fi initiatives in India.

Prior to the infamous terror attacks of 2008, the use of Wi-Fi services in India was largely unregulated. However, once it was discovered that the perpetrators had made use of multiple unsecured Wi-Fi networks to co-ordinate their attacks,[2] the Department of Telecommunications

1 Available at http://trai.gov.in/WriteReadData/WhatsNew/Documents/Press_Release_No.22.pdf , last accessed on August 22, 2016.

2 *TRAI plans to prevent Wi-Fi abuse*, The Economic Times, September 17, 2008, available at: http://articles.economictimes.indiatimes.com/2008-09-17/news/28383193_1_isps-wifi-connections-internet-service-providers, last accessed on August 22, 2016

(DOT) issued a set of instructions[3] in 2009 to all Internet Service Providers (ISPs) operating under the Unified Access, Cellular and Mobile Telephone, and Basic Service Licenses (UASL, CMTSL, BSL), directing them to adhere to certain procedural mandates designed to bring greater security and accountability to the use of Wi-Fi networks within India. Among said mandates is the identity verification of Wi-Fi users either by retaining copies of their photo IDs, or by delivering login details via SMS, thus retaining their phone numbers as a means of identity verification. It is important to note that these instructions issued by DOT apply to ISPs licensed under the UASL, CMTSL, and BSL and their franchisees, which means the ISPs are also bound by the numerous general, operating, financial and security conditions contained therein, including but not limited to maintaining detailed registers identifying their customers, and maintaining logs of all data packets transmitted to and from customer-premise equipments.

While the above-mentioned instructions from DOT remained the sole governing framework for public Wi-Fi initiatives for some time, the Information Technology (Guidelines for Cyber Cafe) Rules (hereinafter, the Cyber Cafe Rules) introduced in 2011 added another potential regulatory layer by virtue of their definition of the term "cyber cafe"[4] in a manner that proved broad enough to encompass public Wi-Fi providers. The Cyber Cafe Rules, like the DOT instructions, were introduced in the aftermath of the 2008 terror attacks, and sought to bring in a measure of accountability to the use of cyber cafes across the nation. As such, the Rules require cyber cafes to compulsorily register themselves with a Government agency, procure and maintain logs of customers' identification documents, and abide by specific stipulations as to the physical layout of computer resources installed on their premises for use by customers. Unlike the DOT instructions however, the application of the Cyber Cafe Rules is not limited to ISPs licensed by the DOT, and extends to every public Wi-Fi provider – be it a licensed ISP, a data reseller, a data aggregator, or even a small business owner broadcasting a Wi-Fi network for public use around his/her premises.

The parallel operation of the above two regulatory frameworks lead to substantial ambiguities with respect to provision of public Wi-Fi services by licensed ISPs as opposed to non-licensed providers. For instance, for public Wi-Fi networks operated by licensed ISPs in accordance with the DOT instructions, identity verification of customers may be done either by retaining copies of photo IDs

3 Department of Telecommunications, *Instructions under the UASL/CMTS/BASIC Service Licence regarding provision of Wi-Fi Internet service under delicensed frequency band*, February 23, 2009, available at: http://www.dot.gov.in/sites/default/files/Wi-%20fi%20Direction%20to%20UASL-CMTS-BASIC%2023%20Feb%2009.pdf, last accessed on August 22, 2016

4 "Cyber cafe" is defined under Section 2(1)(na) of the Information Technology Act, 2000 as: *any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public*

or by provisioning logins via SMS to registered mobile numbers. For non-licensed Wi-Fi providers like a small business owner on the other hand, identity verification through mobile phone numbers is not an option under the Cyber Cafe Rules. Further, if one were to assume that the Cyber Cafe Rules are interpreted in such a manner as to exclude public Wi-Fi services from their ambit (seeing how the legislative intent was clearly to regulate physical cyber cafes as opposed to every Internet service point that is captured by broadness of language), then Wi-Fi services offered by non-licensed ISPs would be left in a regulatory grey area at best, and unregulated at worst.

In order to resolve the above-mentioned regulatory ambiguities, both the DOT instructions and the Cyber Cafe Rules need to be revisited, and the respective subjects of these regulatory frameworks, as well as their roles and responsibilities must be elaborated in greater detail.

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?

Regulatory and policy measures must focus on the following broad areas in order to encourage the comprehensive deployment of public Wi-Fi networks in urban as well as rural areas:

- *Privacy and security concerns:* It has been observed that people harbor apprehensions about using public Wi-Fi services as they do not understand how their personal data is being handled. Neither the DOT instructions, nor the Cyber Cafe Rules lay down minimum security standards to be incorporated into the public Wi-Fi offerings themselves or to the database of identity documents collected. Both regulatory frameworks also refrain from mandating the destruction of identity documents after their respective retention periods. As a result, there exists a level of mistrust between the Wi-Fi providers and customers, as customers are unable to trust Wi-Fi services rendered, and Wi-Fi providers are forever fearful of liability arising from fake identification documents.[5] In the absence of any overarching law on data protection in India, we recommend that applicable regulations be updated to address the privacy concerns, use of secured Wi-Fi, handling of the users' personal data, and the liability of Wi-Fi providers.

5 Behdad Mahichi, *India: Unlocking public Wi-Fi hotspots*, April 20, 2016, availabe at: http://www.aljazeera.com/indepth/features/2016/03/india-unlocking-public-wi-fi-hotspots-160308072320835.html, last accessed on August 21, 2016

- *Cost concerns:* The need to readily identify a person is not just cumbersome but also expensive. Companies that help establish authentication portals can charge hefty prices, which may render public Wi-Fi a prohibitively expensive area of engagement for smaller businesses and individuals.[6] Thus, apart from bigger players such as Starbucks, KFC or McDonald's who have the financial capabilities to provide a connection with proper authentication, it creates a barrier for smaller businesses, cafe owners or independent players to provide public Wi-Fi as add on service to their exiting businesses.

- *Lack of awareness:* There is a lack of awareness and general digital literacy that has hindered the growth of Public Wi-Fi. Actually connecting to a Wi-Fi network may prove difficult for anyone who is not well acquainted with the technology, and this is a problem prevailing not only in the cities but also rural areas.[7] For instance, people traveling from rural areas may be entirely unaware of the existence of public Wi-Fi networks in certain railway stations, and even if they were aware, might lack the technical know-how to make use of the facilities.[8]

- *Environmental Issues:* This is specially prevalent in older cities where issues related to electricity shortages, badly planned and jam packed cities or in some cases even wild animals which make it very tough to make public Wi-Fi available at the street level. Electricity shortages or power cuts, especially in small cities and towns directly affects connectivity through technologies like Wi-Fi which cannot operate without reliable power sources. Jam packed and older cities also create problems as it becomes difficult to lay cables or fiber optics where everything is already built up. In certain cases, apart from the issues already mentioned, additional problems also emerge such as monkeys that feast on fiber-optic cables.[9]

Thus, in order to expand and 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, the following steps can be taken:

- Update current regulations in context of public Wi-Fi providers and users to address the

6 Ibid.
7 Meghna Rao, *Think it's hard finding free wifi in India? This app says think again*, March 22, 2016, available at: https://www.techinasia.com/free-wifi-app-india, last accessed on August 21, 2016
8 Ibid.
9 Reuters, *Problems with street-level Wi-Fi in India: power cuts, congestion — and monkeys*, April 2, 2016, available at: http://www.firstpost.com/business/problems-street-level-wi-fi-india-power-cuts-congestion-monkeys-2183931.html, last accessed on August 21, 2016

privacy concerns, use of secure Wi-Fi, handling of the users data and the liability of Wi-Fi providers, so as to foster a positive regulatory environment for encouraging and boosting Wi-Fi growth in India.

- It is also recommended that the different entities providing Public Wi-Fi such as bigger businesses or even small cafes should be given tax subsidies by the government to further incentivize them to provide public Wi-Fi.
- There must be renewed focus on initiatives such as the National Digital Literacy Mission, with learning modules dedicated to accessing and effectively utilizing public Wi-Fi services. Beneficiaries must be given hands-on training and assisted in navigating Wi-Fi networks and the Internet in general.
- Emphasis must be laid on bolstering support-infrastructure including uninterrupted power supply, and all assistance must be provided in expanding Internet penetration, for instance by expediting the provision of clearances necessary to lay network cables. Assistance may also be provided in maintenance of existing infrastructure and securing it against environmental adversities.

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

In context of encouraging interoperability between Wi-Fi networks of different service providers, we invite the Authority's attention to an initiative jointly launched in 2012 by five of the six largest Multiple-Systems Operators (MSO) in the United States, namely Bright House Networks, Cablevision, Comcast, Cox Communications and Time Warner Cable (known collectively as the CableWiFi Consortium).[10] As per the terms of this alliance, subscribers of each cable Internet provider are allowed to roam freely among the 250,000-odd “CableWiFi” hotspots that are owned and operated nationwide by the Consortium. Subscribers connect to a Wi-Fi access point using the same credentials they use to join their respective MSOs' Wi-Fi networks, and once a device is authenticated, users will auto-connect to a CableWiFi hotspot when they are in range.[11] This results in a single nationwide Wi-Fi network so to speak, where subscribers need log in just once to enable

10 Alan Breznik, *Making the most of Cable WiFi*, September 2014, p. 5, available at: http://www.amdocs.com/products/network-control/Documents/heavy-reading-Wi-Fi-cable-wp.pdf, last accessed on August 24, 2016

11 See http://corporate.comcast.com/news-information/news-feed/cablewifi-alliance-offers-access-to-more-than-150000-wifi-hotspots-creates-largest-wifi-network-in-the-u-s-2, last accessed on August 24, 2016

cross-country Wi-Fi roaming across hotspots operated by multiple service providers.

A similar model may be considered for implementation in India, with Wi-Fi providers coming together to form a commercial consortium and unifying their separate hotspots under a single SSID. The ability to auto-connect and switch seamlessly among hotspots could be enabled on supported devices through the adoption of technologies such as Hotspot 2.0, which makes use of the IEEE 802.11u standard.

However, care should be taken that smaller operators, like those at village level, are not affected due to the interoperability measures. The smaller service providers should be allowed to exist independently of such interoperability requirements considering the overheads that could be associated with such requirements. This will be important to ensure that the village wi-fi networks are affordable.

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.

In India, a large part of spectrum is regulated by the Government. The Supreme Court of India in *Union of India v. Cricket Association of Bengal*[12] declared that the use of airwaves "has to be controlled and regulated by a public authority in the interests of the public and to prevent the invasion of their rights." However, there exist large spectrum bands that could be utilised in public interest like the UHF band used for TV transmission.

The Central Government has an ambitious plan to ensure high-speed connectivity upto the Panchayat level using the National Optic Fibre Network. However, to ensure optimum use of this bandwidth, middle mile and last mile connectivity needs to be improved. This could be achieved by utilising TV whitespaces for middle mile connectivity up to the village level, and by using Wi-Fi infrastructure for last-mile. [13] For this purpose, white spaces in the TV UHF band (470 - 590 Mhz) will have to be de-licensed. This model will result in stimulating local enterprise and entrepreneurship to operate village level networks. Government could also support such village

12 1995 AIR 1236

13 Kumar Aminesh et. al., *Towards Enabling Broadband for a Billon Plus Population with TV White Spaces*, March 2016, available at: http://arxiv.org/pdf/1603.01999v1.pdf, last accessed on August 23, 2016

level networks by providing affordable subscriber authentication systems built using Free and Open Source Software (FOSS) and general purpose hardware. We have proposed one such village level network in our answer to Question 12.

De-licensing spectrum would lead to innovation and entrepreneurship as there will be fewer regulatory and barriers. This could also lead to lowering costs of data plans of mobile services due to increased competition.[14] In this regard, Canada has been very successful in utilising TV white spaces to improve broadband coverage in rural areas through its Remote Rural Broadband Systems(RRBS) initiative. [15]

Apart from what has already been recommended by TRAI, such as de-licensing spectrum, use of frequency bands such as 57-64 Ghz (V band) & 71-76 Ghz & 81-86 Ghz (E band), and use of TV White Spaces; we would like to recommend that the frequency band of 5470-5725 Mhz (U-NII Worldwide) should be de-licensed. It should be open for both outdoor and indoor use, subject to Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) capabilities. This spectrum was added by the Federal Communications Commission of United States (FCC) in 2004 to "align the frequency bands used by U-NII devices in the United States with bands in other parts of the world".[16] Other international examples include Germany, which has also de-licensed this frequency band, for both outdoor and indoor use, subject to DFS and TPC capabilities. Since this is the German implementation of European Union Rule 2005/513/EC, similar regulations could be expected throughout the European Union.[17][18] South Africa has also modeled its laws based on the European regulations[19] and Brazil has also de-licensed this frequency band subject to DFS.[20]

14 Paul Milgrom, Jonathan Levin and Assaf Eilat, *The Case For Unlicensed Spectrum*, October 12, 2011, available at: https://web.stanford.edu/~jdlevin/Papers/UnlicensedSpectrum.pdf, last accessed on August 23, 2016

15 Licensing procedure for Remote Rural Broadband Systems, CPC-2-1-24, available at: http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10062.html, last accessed on August 20, 2016

16 Federal Communications Commission, *Unlicensed Devices in the 5 GHz Band*, 69 FR 2677, January 20, 2004, available at: https://www.federalregister.gov/articles/2004/01/20/04-1126/unlicensed-devices-in-the-5-ghz-band, last accessed on August 21, 2016

17 *European Commission Decision on the harmonised use of radio spectrum in the 5 GHz frequency band for the implementation of wireless access systems including radio local area networks (WAS/RLANs)*, 2005/513/EC, July 11, 2005, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32005D0513, last accessed on August 21, 2016

18 *European Commission Decision amending Decision 2005/513/EC on the harmonised use of radio spectrum in the 5 GHz frequency band for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs)*, 2007/90/EC, February 12, 2007, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007D0090, last accessed on August 21, 2016

19 Electronic Communications Act, 2005 Regulations, availabe at: http://www.ellipsis.co.za/wp-content/uploads/2008/07/licence_exemption_frequency_regs_2008.pdf, last accessed on August 22, 2016

20 Resolution No. 506, July 7, 2008, available at: http://www.anatel.gov.br/legislacao/resolucoes/2008/104-resolucao-506, last accessed on August 22, 2016

In conclusion, we submit that de-licensing and use of frequency bands 5470-5725 Mhz (U-NII Worldwide) & 470-590 Mhz (TV UHF Band) has the potential to further bridge the digital divide, foster innovation and competition, complement traditional access and help in further improving broadband penetration.

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?

&

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 to Wi-Fi services?

The facilitation and proliferation of public Wi-Fi hotspots is hindered primarily by two interlinked concerns; one, a secure means of identifying the users of the platform, and second, a simplified payment mechanism to compensate the service provider. This answer will initially highlight the objectives of these two mechanisms in brief to set the context, then move onto the challenges faced in their uniform application, and subsequently lay out our suggested alternatives to circumvent these concerns.

The foremost objective of a login/authentication system is to maintain a catalog of users to counteract the past experiences that raise concerns regarding misuse of a public Wi-Fi system that is openly accessible to all, without any mechanism to register their identity. However, where there is a valid requirement for such a system, the existence of a vast range of service providers at the local and national levels, and the differing categories of user base; pose a challenge for devising a model that will achieve uniform applicability. One of the most commonly implemented methods in this regard is the OTP (One Time Password) method of authentication, where the mobile number of the user is recorded as a means of identification, and the subsequent usage of the Wi-Fi service is enabled upon the successful authentication through the one time password sent on the registered mobile number. Although, it is recognized that mobile phone penetration and usage of Internet services through mobile phones is substantially higher in the country as opposed to broadband services, or use of Internet on other devices[21]; the OTP method excludes and is unusable for the

21 Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators for January to*

category of individuals that do not have a valid telephone number in the country, or access to a mobile phone at the time. Therefore, a common identifier or measure that is not limited by the proximity of a mobile phone/number should be considered.

The second issue involved in tandem to the login/authentication of users is the effective implementation of a payment system that caters to the revenue of the service providers. Most of the current public Wi-Fi models operate on a short time quota of free Wi-Fi services, at the expiration of which, they are upgraded to a paid service. There have been studies by various service providers that state that there is a steep dip in the percentage of people who use public Wi-Fi services post the free of cost time frame.[22] The challenge at this stage is two fold; first, to provide a sustainable model of revenue generation for service providers who invest in the creation and maintenance of public Wi-Fi hotspots, and second, to ensure that this model is inclusive in its nature and can have a horizontal application across the diverse social, economic, and developmental backgrounds in the country, and does not limit its functioning to online transactions.

For a public Wi-Fi system to be sustainable, the identification data of the user needs to be processed in a secure system with requisite data protection safeguards to ensure the privacy of an individual, along with ensuring a method that can serve as an incentive for the service providers to invest in developing and maintaining these hotspots. A few suggestions that reconcile the above-mentioned challenges with both of these issues are given below:

1. Recharge Model: Under this system, recharge coupons for the required amount of data can be purchased from brick & mortar stores or through online platforms. By extending the facility to physical vouchers that can be purchased from physical stores that usually cater to other mobile and data recharges, this model eliminates the restriction of online transactions for upgrading the public Wi-Fi post the free quota. These vouchers can either be ISP specific, i.e. cater to the hotspots being provided by that particular service provider, or be uniform across the city/town/village to enhance the utility of these vouchers. Where the former model would be more applicable to a city that will have multiple service providers catering to different parts of the city; the latter model might be suitable for a small town where the entire public Wi-Fi system is being maintained by one service provider. A small

March, 2016, Executive Summary, p. v, August 5, 2016, available at: http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator_Report_05_August_2016.pdf, last accessed on August 24, 2016

22 *Wi-Fi hotspots in Kochi not generating traffic*, The Hindu, August 24, 2016, available at: http://www.thehindu.com/todays-paper/tp-national/tp-kerala/wifi-hotspots-in-kochi-not-generating-traffic/article9024112.ece, last accessed on August 24, 2016

scale successful example of this model is a small village of Bhadra in Rajasthan[23] that is entirely covered by public Wi-Fi being provided by MTS. MTS has developed data packages (for example, Rs 64 for 1 GB of data)[24] with ID & password, where public Internet can be accessed in accordance with the volume of data bought.

Moreover, with respect to simplifying the authentication/login process, the physical brick & mortar stores can maintain documentation of mobile numbers or other acceptable ID proofs [as mentioned in the DOT instruction and the Information Technology (Guidelines for Cyber Cafe) Rules, 2011] in a digitized format. Also, when using the option of pre-ordering these vouchers online, an OTP or email confirmation format should cater to the needs of both, domestic and foreign users. Therefore, this model has the potential to overcome the challenges posed by both, authentication of users, and payment generation for service providers.

2. Advertisement Model: This model is based on the initiative being run by Muft Internet[25], a multidimensional enterprise that aims to proliferate Internet access and use and facilitate last mile connectivity. Under this method, the user has to watch advertisements for a short duration to attain free access to the Internet for a stipulated time, the cycle can be repeated to increase the duration of Internet access. With the help of this scheme, as per Muft Internet, one is able to access one hour worth of Internet services by watching an advertisement for 15 seconds.[26] Therefore, service providers source their revenue by collaborating with advertisers, and grant access to the public Wi-Fi hotspots to users for a set amount of time.

   The authentication function under this model can be chosen from a host of variants, like an OTP (for users who have a valid domestic phone number), or a connected service that generates an access code upon pre-registration through email address (for foreign or domestic users).

3. Deduction through mobile carrier billing: In yet another model that can ease the payment challenges, we suggest a method that enables a user to access public Wi-Fi by any service

23 Kalyan Parbat, *How Wi-Fi is transforming lives in Rajasthan's Bhadra*, Economic Times, August 1, 2015, available at: http://economictimes.indiatimes.com/tech/internet/how-wi-fi-is-transforming-lives-in-rajasthans-bhadra/articleshow/48302716.cms, last accessed on August 23, 2016

24 Subhajyoti Ghosh, *India's only town with full public Wi-Fi*, BBC News, October 26, 2015, available at: http://www.bbc.com/news/world-asia-india-34462435, last accessed on August 23, 2016

25 See http://muftinternet.com/, last accessed on August 23, 2016

26 Muft WiFi Network, Community powered Wi-Fi zones; Muft Internet, available at: http://muftinternet.com/#sectionid-715; last accessed on 23rd August, 2016

provider, through an OTP authentication process, and the determined cost per the usage of public Wi-Fi services can be billed by their mobile carrier to their phone account. The hurdle for successful implementation of this model would entail an agreement between all the public Wi-Fi service providers and Telecommunications Service Providers (TSPs) with respect to the per unit cost of data that is used through public Wi-Fi networks and form a uniform billing structure. However, this model will only function through an OTP regulated login process as a valid domestic mobile number would be the operative element of this system.

For a frictionless use of a public Wi-Fi network, we understand that the possible solution is a central authentication and payment system that can be used by domestic users across the country, and also caters to foreign visitors by a valid passport number authentication. In this regard, the usage of Aadhaar, and the Unified Payment Interface (UPI) has been suggested in the Consultation paper by TRAI to formulate this centralized hub for the above discussed concerns. However, with the current restrictions that surround the use of Aadhaar due to the Supreme Court order dated 15th October, 2015, its usage is limited to only six government schemes, namely- PDS, LPG, MNREGA, PM Jan Dhan Yojna, National Social Assistance Program, and Employees' Provident Fund Organization (EPFO).[27] Although the Aadhaar (Targeted Delivery of Benefits & Subsidies) Act, 2016 has received President's assent, only a portion of it has been notified by the Central Government till date.[28] Apart from the pending Supreme Court challenges to this scheme on various grounds, including a lack of a foundational framework with adequate privacy and security safeguards, the Aadhaar Act, 2016 has also been criticized for not incorporating sufficient clauses that ensure a secure collection, usage, and storage of the biometric data of individuals. To illustrate, the Act does not make it mandatory for the enrollment agency to notify the individuals about the security standards and protocols being followed by them while collecting the data, or being followed in the central database for storing such sensitive data. Furthermore, although the Act permits the UIDAI to keep a record of authentications made on the basis of the Aadhaar number or biometrics, it fails to specify a retention period for such records.[29] Also, owing to the increase in data hacks and breaches

27 K.S. Puttaswamy & Ors. v. Union of India & Ors. (W.P.(C) 494/2012), Supreme Court order dated 15th October, 2015; available at: http://sflc.in/wp-content/uploads/2016/05/15th-October-2015.pdf; last accessed on 24th August, 2016

28 Aman Sharma, *Government notifies Aadhaar Act, forms panel to choose new chief of UIDAI*, Economic Times, 13th July, 2016; available at: http://economictimes.indiatimes.com/news/economy/policy/government-notifies-aadhaar-act-forms-panel-to-choose-new-chief-of-uidai/articleshow/53183308.cms; last accessed on 24th August, 2016

29 SFLC.in, *Evaluating the Aadhaar Bill against the National Privacy Principles*, 11th March, 2016; available at: http://sflc.in/evaluating-the-aadhaar-bill-against-the-national-privacy-principles/; last accessed on 24th August, 2016

all across the globe, there have been apprehensions regarding the security of a central database with personal sensitive information, and other data of almost one billion people. Therefore, with the valid privacy and security concerns that surround this scheme, implementing Aadhaar as a central point for authentication for public Wi-Fi networks all across the country should not be considered. Moreover, as mentioned above, the entire Aadhaar Act has not yet been notified by the Central Government and in its absence, the above mentioned Supreme Court order restricting the use of Aadhaar to six schemes and making its usage voluntary, is applicable on the operation of the Aadhaar scheme.

In the absence of the combination of Aadhaar and UPI to create a centralized hub, we recommend a simultaneous application of the above suggested alternate models that have the ability to collectively remedy the various challenges posed by both, the authentication and payment requirements for a public Wi-Fi system.

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?

To promote hosting of data of community interest at local level, we propose establishment of a Municipal Area Network (MAN) based on our 'Broad Strokes Proposal'.[30] This proposed initiative focuses on initially building a network to interconnect the people and important public institutions in a city, town or village over high-speed connections. Such a network can provide many of the same benefits as a broadband public Internet access service with a drastically lower need for backhaul Internet bandwidth. Moreover, it can host information of community interest, thereby immensely benefiting the consumers and reducing the cost of data for them.

Such a network can be rolled out in a phased manner:

- *Laying Foundation and Connecting Civic Centers:* At the foundation, a MAN can comprise of a network that links together civic centers of the community such as government offices, police and public safety stations, schools, and other important institutions. Each node in the MAN could be linked with a high-speed connection appropriate to the circumstances by considering and taking into account various factors such as geographical location of the place, and existing infrastructure, and could vary from fiber-optic cabling, high-bandwidth

30 SFLC.in, *Comments on The Delhi Government's Public Wi-Fi Initiative*, available at: http://sflc.in/wp-content/uploads/2015/06/Comments_DelhiPublicWiFi-12.pdf, last accessed on August 23, 2016

mid-range point-to-point wireless equipment or whitespace “super Wi-Fi” technologies or by even employing the Hotspot 2.0 technology[31]. Through virtual network tagging, these wireless hot-spots or hot-zones can provide both secure managed access to Government resources for Government employees and open access to a public network for everyone with a Wi-Fi compatible device in range of a wireless access point (AP). Wireless access to managed Government IT resources from outdoor locations throughout the city, town or village, could allow Government employees who work in the field such as police, emergency workers and inspectors to receive up to the moment information and records without the need to travel back to their individual offices or rely on expensive private cellular wireless services. The next step would be development of government data centers which could offer hosted content and services for government offices and other institutions on the network and other data of community interest for example locally hosted mirrors of not-for profit public interest educational websites such as Wikipedia or Khan Academy.

- *Civic Expansion:* Once the above mentioned foundation network is in place and being used by the public, the MAN can be further expanded to include new areas which were not covered before, for example public parks and similar public meeting places by establishing nodes and Wi-Fi hot-zones. As MAN expands to these locations, its utility will grow exponentially by connecting more people to more valuable resources and significantly reduce their cost as all of these resources and data are hosted locally. Moreover, it can be resourceful by providing more opportunities collaborate and share, which in turn will enable improved research, tele-medicine, and public access to health, safety and educational materials.

As a general matter, we encourage the use of commodity hardware, open standards and free and open source software (FOSS) wherever possible and with a particular emphasis on the network's edges. A preference for these kinds of technologies is motivated by factors such as security, flexibility, longevity, cost, and lock-in risk. The openness of these tools provides an opportunity to involve students, businesses, and community groups in developing innovative new tools and valuable experience in the area of network and computer technology. One potential use for these technologies is that it allows for innovations such as ad-hoc extension of the MAN. Community wireless networks based on mesh or other wireless network technologies can be surprisingly

31 Prasid Banerjee, *The future of public WiFi in India and the world*, January 14, 2016, available at: http://www.digit.in/internet/the-future-of-wifi-in-india-and-the-world-28639.html, last accessed on August 23, 2016

effective. The Freifunk project that is based on the OpenWrt router firmware, and uses open mesh wireless standards such as OSLR and B.A.T.M.A.N., is an example of a community mesh wireless initiative with multiple network deployments. The openness of these tools provides an opportunity to involve students, businesses, and community groups in developing innovative new tools and valuable experience in the area of network and computer technology.

Question 13: Any other issue related to the matter of consultation.

The consultation paper has been quite comprehensive in terms of recognizing and outlining various issues that have an impact on the working of public Wi-Fi network in India. A few significant issues that were highlighted are regulatory issues, login/authentication procedures, payment gateways, to name a few. However as important these issues are, there is a complete lack of focus on issues concerning privacy and data protection, and how these issues affect various users who access the huge public Wi-Fi network that the government intends to deploy. While the core component of this consultation paper is its focus on the model that can be used for deployment of a large scale public Wi-Fi network throughout India, it is increasingly important that this system be based upon foundations that safeguard privacy and security of the users' data.

As we've already pointed out in our previous answers above that apart from there being an ambiguity in the current frameworks surrounding public Wi-Fi, neither the Information Technology (Guidelines for Cyber Cafe) Rules, 2011, nor the DOT instruction of 2009, lay down minimum security standards to be incorporated to the database of identity documents collected nor do they mandate the destruction of these identity documents after the retention period of a year is over. This has led to the general public becoming apprehensive towards using public Wi-Fi networks due to the lack of transparency about the processing of personal data.

The working of this public Wi-Fi system entails processes that include the handling of personal information of users in the form of login/authentication data, as well as the data that accounts for usage of various services over the public Wi-Fi networks. Although, there are certain provisions under the Information Technology Act, 2000 that attempt to protect and safeguard processing of data, their limited scope of application deems these clauses insufficient to qualify as the data protection regime for the country. To illustrate, with respect to personal data, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 merely mandate the existence of a privacy policy with certain clauses, but

fails to expand on the principles that need to be followed for the collection, storage, use, access of the data provided by the user.

Even though there have been efforts towards drafting a privacy legislation, an ongoing process for the past 6 years no concrete bill has been laid down in front of our Parliament for consideration. Therefore, the Indian legal system lacks a comprehensive data protection framework that lays down the rights of the users with respect to their data, responsibilities of the data handlers, clear details about security and encryption protocols, or transparency and accountability measures.

A successful public Wi-Fi network deployed on a mass scale will have to ensure the security and privacy of not only users' personal information that is used for login purposes, but also be mindful of safeguarding the content that is accessed by users' over these public Wi-Fi networks. With the Government rolling out initiatives like Digital India to promote the digital culture and its proliferation across the country, the digital footprint of every user, in rural or urban areas, is expanding substantially. Therefore, with India being the biggest contributor of the next billion people on the Internet, it is imperative that the development and deployment of a public Wi-Fi network on a large scale be built on the strong foundations of privacy and security, which will be dependent on the establishment of an over arching, all encompassing data protection regime.