RESPONSE TO TRAI CONSULTATION PAPER NO: 14/2016

ON

PROLIFERATION OF BROADBAND THROUGH PUBLIC WI-FI

By: Anandapadmanabhan Unnikrishnan
Sharwari Pandit
Swapnasarit Sathpathy
Abhishek Rao

Panel Constituted by the Law and Technology Society,
National Law School of India University.

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY,
BANGALORE

Table of Contents

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?

We, currently reside in a society where there is a substantially high demand for enhancement in digital connectivity and as a consequence, there is a burgeoning demand for Public Wi-Fi services. There are currently over 31,000 public Wi-Fi hotspots installed in India, according to industry estimates, and the number is expected to grow beyond 202,000 by 2018. However, for India to match the current global average of one public Wi-Fi hotspot per 150 people, an additional 800,000 hotspots need to be deployed.[1] Thus, India is lagging behind the global growth rate substantially insofar as the expansion of Public WiFi is considered.

One of the contributing factors which has stalled the expansion of public Wi-Fi networks is that there exist operational issues such as discontinuous (non-seamless) and discouraging consumer user experiences due to Wi-Fi user authentication regulations. The Department of Telecommunications (DoT), Government of India, brought about regulations which laid down the procedure for secure use of public WiFi.[2] The DoT regulations were in the wake of recent terrorist events in India that exhibited how easily, unsecured WiFi networks can be misused and can

1 Jayanth Kolla, Future of public Wi-Fi hot spots in India, available at http://www.livemint.com/Consumer/Uc506lrKsLh4TYllnqPcdO/Future-of-public-WiFi-hot-spots-in-India.html.

2 Regulation (dated February 23, 2009) Available at http://www.dot.gov.in/sites/default/files/Wi-%20fi%20Direction%20to%20UASL-CMTS-BASIC%2023%20Feb%2009.pdf.

endanger national security.[3] The underlying objective of the DoT regulation was to ensure that public WiFi Internet access are not utilised for illegal purpose and to be able to track down the perpetrator in case of abuse.[4] To this effect, DoT had instructed all ISPs to enforce centralized authentication using LoginIDs and Passwords for each user. It mandates that all Wi-Fi owners have to secure their networks with a password, to keep a record of their users in one of two ways: by keeping a record of the customer's data usage as well as their photo identification for a period of one year; or the owners could set up an authentication portal that automatically collects the data of the user's activities. Due to these regulatory measures, a number of Service Providers are hesitant to expand which has affected the growth.

In India, public Wi-Fi has also not been able to grow at a rate keeping in pace with the global growth rate and for consumers, it is not easy to use due to cumbersome payment methods. Currently, there is no centralized mechanism for payment across networks, making it a cumbersome process for a user to pay for each hotspot as they move from one place to another. There are no regulatory measures with respect to a unified payment system which results in inconvenience to the users due to the lack of such a system, and has been detrimental in stimulating demand.

Spectrum de-licensing in case of Public Hotspots is a flexible approach to spectrum management, which fuels innovation and market development. When it comes to licensing, there should be more unlicensed spectrum in the 2.4 GHz range, exceeding the range of what is already unlicensed, which will contribute majorly towards expansion of wireless networks.[5] In countries like US and UK, regulators have freed up more spectrum bands for license-exempt use to fuel the use of such public Hotspots.[6]

Although ideally, the Government will be keen to avoid overburdening such providers of public Wi-Fi with regulatory compliance measures taking into consideration the several advantages that

---

3 Behdad Mahichi, India: Unlocking public wi-fi hotspots, available at http://www.aljazeera.com/indepth/features/2016/03/india-unlocking-public-wi-fi-hotspots-160308072320835.html.

4 Hemant Chaskar, Complying with DoT Regulation on Secure Use of WiFi: Less in Letter, More in Spirit, available at http://www.mojonetworks.com/fileadmin/pdf/Implementing_DoT_Regulation_on_WiFi_Security.pdf

5 Unlicensed Spectrum, Center For Internet & Society, available at http://cis-india.org/telecom/unlicensed-spectrum-brief.pdf.

6 Ofcom Infrastructure Report 2014,106, available at http://stakeholders.ofcom.org.uk/binaries/research/infrastructure/2014/infrastructure-14.pdf.

the proliferation of public Wi-fi services can provide to the community and the business sector, this has to be necessarily weighed against the need to regulate the domain in order to protect data privacy, counter organised crime and check online infringement of intellectual property rights. As public Wi-Fi networks and their use expands, so does the threat of misuse, making it imperative to have some sort of regulatory regime in place.

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?

There exists a huge divide when it comes to access to internet and internet infrastructure. Community wireless networks using unlicensed frequencies have the potential to provide marginalized communities with low cost and accessible sources of local information, as well as connection to the rest of the world at an affordable cost. Such networks can facilitate initiatives like telemedicine, e-governance, e-commerce, e-learning, and telephony services through Voice over Internet Protocol (VoIP) at a much lower cost.

It might prove to be incredibly difficult and unfeasible to undertake and support the substantial amount of investment that will be required in order to expand WiFi networks in rural areas since it's generally not a lucrative or profitable business proposition in these areas. Taking into consideration the budgetary constraints of the state, it becomes a necessity to involve the private sector to participate in the mission to ensure universal access to internet services. The small population in a typical rural area or community does not make for a good consumer base since it does not promise a guaranteed and sustainable potential return for the required investments.

Most of the Indian telcos provide enterprise Wi-Fi solutions through custom deployments in IT and business parks, educational institutes (campus Wi-Fi), hospitals, etc. They have not ventured into community Wi-Fi networks or urban location-aware services. It is imperative that a common ground is achieved by which private interest will interoperate with public interest to provide public

goods.[7] In order to make the market effective for the private players, the government need to provide incentives to private players by taking such steps so as to reduce the operational costs as well as other transaction costs as insofar as market entry is concerned. With the reduction of costs associated with market entry, competition will be bolstered which would result in lesser costs being passed down to the users.

Since the marginal return from investment in deployment of such Wi-Fi networks is smaller in rural areas as compared to urban areas, certain incentives have to be bestowed upon the providers. Certain manners in which such deployment of Wi-Fi networks could be encouraged in rural area is by granting of tax holidays to such interested service providers for a specific time limit. Such incentives could take the form of a spectrum set-aside, financial subsidies, reduced auction fees, smaller tier sizes and measures to prevent the hoarding of spectrum.[8] Since ISPs and telecom companies make their own investment in setting up public WiFi services, certain incentives must be provided to ISPs and Wi-Fi providers, such as Right of Way permissions, permission to setup kiosks at select locations to promote Wi-Fi services benefitting the entire community etc.

Insofar as the demand component is concerned, the state can stimulate the demand for public Wi-Fi infrastructure by rolling out more E-Governance schemes that would encourage the use of internet networks to access such applications.[9] The state should also resort to utilise such Wi-Fi networks as means to deliver government services to the rural population enhancing the demand for such usage. Thus, the key lies in developing government initiatives and programs that would encourage the aggregation of demand. However, it is equally important that the rural users and businesses possess the knowledge of how to effectively use the technology, if such knowledge is lacking, the investment in infrastructure is of very little use. Government must undertake programs which can play a critical role in educating rural constituents about the various benefits that can be harnessed using public WiFi networks.

---

7 Idongesit Williams, Telecom Policy Innovation: the Role of Free Spectrum and Telecommunication Development in Rural Ghana, Vol. 6(3), Journal of Technology Management & Innovation, (2011).

8 Spectrum Management and Telecommunications, available at http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10124.html.

9 Policy Alternatives For Deployment of Broadband Services in Rural Areas, available at http://esd.ny.gov/Resources/broadband.pdf.

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?

A. The most significant problem faced in providing Wi-Fi in public spaces is the unsuitability of any of the current mechanisms to provide a uniform, seamless system to permanent users of ISPs, temporary users with domestic numbers and users with numbers from foreign providers. The current challenges, as identified by the paper and other sources, include the inability of the network to support a large number of people, the extensive delays in handing out OTPs and the inability of foreign persons to register on the network, etc.[10]

Among the multiple options considered in the paper, the first one which can be argued against is the proposal to link the verification process and provision of a login id and password to AADHAR Cards. The first reason is the lack of complete coverage of the AADHAR Card among the Indian populous. Further, the AADHAR Card, not being compulsory as of now, cannot be the sole form of identification allowed for Wi-Fi access in public areas. Lastly, it would require the members to carry their AADHAR Card with them at all times, and ensuring secure and proper use of the same will prove immensely challenging.[11]

10 TRAI Consultation Paper on Proliferation of Broadban Through Public Wi-Fi Networks, p.25.
10 See, Critique of the AADHAR d Through Public Wi-Fi Networks, p.25.
11 See, Critique of the AADHAR Bill On Multiple Issues, Center for Internet and Society, available at http://cis-india.org/aadhaar-bill-2016.

The best solution would be to create a two-fold categorisation of customers, and create systems accordingly –

- **For Domestic Customers**

Regardless of whether they are ad-hoc or permanent subscribers of the service provider, creating a temporary login and password, based on an OTP system is preferable. First, it removes the need for the creation of a separate permanent ID system for the use of subscribers, reducing the load of creating, maintaining and verifying these accounts. Second, due to multiple providers being subscribed to in India, unless we adopt a central platform which hosts all these providers, and then allow each of them to create permanent accounts, inter-operability will be hard to achieve.

Another option could be to enable something similar to the Elitecore – TTSL Wi-Fi Plan,[12]wherein Wi-Fi can be enabled by operators at public places with highest footfalls, including airports, railway stations, etc. There are multiple options for their operator and non operator users. For the operators' users, SIM credentials were used for devices which were EAP-SIM enabled (purchase of SIM card in India requires provision of a photo identity proof, which must be shared by the SIM provider with the government in accordance with current regulations and agreement). In case of operators' existing users without an EAP-SIM enabled device, they can be redirected to a captive portal and mobile number and OTP can be used to login. However, captive portals can be exceedingly cumbersome, interrupt surfing repeatedly, and often fail to function/function extremely slowly in case of excessive burden due to multiple persons accessing it. The Plan also provides online vouchers (through online payment) or physical scratch card vouchers for Wi-Fi access. However, the inherent limitation here is that it will be limited to individual operators. The use of physical scratch cards or online vouchers may be especially useful to cater to foreign customers.

12 Elitecore TTSL Wi-Fi Case Study, available at http://worldwifiday.com/wp-content/uploads/2016/06/Elitecore-Wi-Fi-SMP-case-study-Enables-Tata-Teleservices-Ltd.-to-roll-....pdf.

- **For Foreign Customers**

According to the letter released by the DoT, Wi-Fi access can be granted to persons post identification using a photo identity card (the copy of which must be kept for up to a year) or through the provision of a phone number (followed by an OTP, which grants access to the Wi-Fi).[13] For foreign consumers, providing phone numbers which are not registered is not feasible. Hence, allowing the uploading of photo identity to get e temporary login, or to have it shown physically at the Wi-Fi kiosk and an OTP to be granted at the kiosk is another option.

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.

A. Collection of any data which provides financial information, makes it 'Sensitive Personal Data' under the IT (Reasonable Security Practices and Rules), 2008.[14] The collection of this information requires a separate, and higher level of security and safety practices. The first, is the creation of a privacy policy regarding the collection, use and sharing of this information, to be developed by the body corporate/legal entity which collects this information.[15] Depending on the model pursued, either the collecting platform itself, or the individual entities through which the payment will be made, will have to put in place such policies.

Other procedures such as an information and consent page[16] (which is available on almost all

13 Letter to all UASL/CMTS/BASIC Service Providers, Instructions under the UASL/CMTS/BASIC Service License regarding provision of Wi-Fi Internet service under delicensed frequency band, Department of Telecommunications, February 23, 2009, p.3, available at http://www.dot.gov.in/sites/default/files/Wi-%20fi%20Direction%20to%20UASL-CMTS-BASIC%2023%20Feb%2009.pdf.

14 Section 3(ii), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

15 Section 4, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

16 Section 5, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

international public hotspots while accessing paid services) will have to be put in place.

There are multiple concerns which leads to the low subscription for paid public Wi-Fi. The Consultation Paper itself identifies security concerns, logistical hurdles and the inability to carry forward your remaining data usage to any other place as some of the reasons for the low enthusiasm for paid Wi-Fi.[17]

Addressing the first concern, compliance with industry norms for securing data, and collection of only required and approved data is important. This will depend on the payment model finally employed, wherein the responsibility of providing secure payment channels, can be determined and fixed.

The next issues to be considered, that of methods to enable carrying forward of balance data to other places, can be addressed by referring to some common paid Wi-Fi models used internationally. For example, Chicago's O'Hare International Airport provides the option to pay for short, one time only durations of 30 minutes or one hour to longer durations like 30-day plans, wherein the internet can be used for a month at different public locations using Boingo's services.[18] If a similar plan were to be adopted, a monthly access plan for paid Wi-Fi at all public spots wherein a provider provides Wi-Fi can be made available to consumers.

Alternatively, a daily pass model can be put in place, wherein the consumer can obtain a day long pass, or an hourly pass for one device with unlimited use, which will have its own unique login details. However, this would be a manual process. Electronic payment for the same would still involve issues of security and convenience. But, it would remove the need for any differential collection mechanisms for foreign or ad-hoc travelers, and identity proofs or phone numbers can be collected to ensure compliance with the DoT rules.[19]

One of the more uniform policies followed by providers of public Wi-Fi has been to ensure that paid Wi-Fi offers premium services, such as exponentially faster speeds, a seamless and ad-free experience. These are tiered services.[20] As a result, there has been an increase in subscription from a large number of businesspersons and professionals, many of whom require such capabilities.

---

17 TRAI Consultation Paper on Proliferation of Broadband Services in India, p.32.

18 See http://www.flychicago.com/OHare/EN/AtAirport/Facilities/Technology/Pages/Technology.aspx

19 S. Stellin, 'Free Wi-Fi, But Speed Costs', New York Times, (June 12, 2012), available at http://www.nytimes.com/2012/06/05/business/airports-and-hotels-look-at-tiered-pricing-for-internet-access.html?_r=0

20 See http://www.boingo.com/press-releases/dubai-airports-selects-boingo-as-exclusive-airport-wi-fi-provider-2/

The pay as you go plan will require coordination with various service providers, and the higher cost might be a deterrence. However, the wider uniform coverage area will be an added advantage.

Based on the above observation, there is need for a secure centralized payment portal. While the option of purchasing physical daily passes should be kept open for consumers who do not have online payment options, the opening of a centralized payment portal will be highly beneficial for most consumers. Developing such a portal, and allowing the registration of payment agencies/instruments, including online payment wallets (which are preferred by several consumers due to the lack of cumbersome procedures, and ease of payment across platforms) will help to increase subscription. The UPI will allow for these considerations to be taken in, as described in the Consultation Paper. However, the provision of physical coupons which can be paid for by persons without access to payment online or by international travelers (or foreign persons), should be made available.

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?

A. In an ideal scenario, access to public Wi-Fi should be completely delinked from the identity of the user's home network; this would enable all users to access public wireless networks, regardless of any usage entitlements arising out of roaming agreements, thereby increasing the accessibility of the service to the wider public. However, current models are focused precisely on such usage entitlements. For example, in October 2014, AT&T announced that it had entered into an agreement with Accuris Networks and BSG Wireless – both third party network management companies – to market an AT&T branded wifi hub that would enable cellular network operators

to provide access to AT&T's wifi network for their customers.[21] The service, while providing for automated interconnection and seamless interchange between the user's home network (GSM or CDMA as the case may be) and Wi-Fi, relies exclusively on SIM-based authentication. In other words, the hub operates on an opt-in basis similar to data roaming agreements: cellular operators wishing to provide roaming on AT&T's Wi-Fi network are required to "become a part of [AT&T's] the Wi-Fi roaming ecosystem" prior to providing access. Similar offerings from British Telecom, China Mobile and Deutsche Telekom all require[22] cellular operators to enter into 'unilateral interconnection agreements' with the hub operator to provide Wi-Fi roaming to their customers. In essence, this is nothing but old wine in a new bottle (elegant as the new bottle may be).

Ownership and control of the hub would remain with the hub operator. As regards the end-user, the hub operator is virtually in the same position as an independent ISP. Accordingly, the hub operator should be subject to the same regulations applicable to all ISPs, including the Information Technology (Intermediaries Guidelines) Rules, 2011 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011, as well as the TRAI Regulations on Quality of Service for Broadband Service, 2006.

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 payment to obtain Wi-Fi access? Who should own and control such payment platforms? Please give full details in support of your answer.

21 Accuris Networks, AT&T Mobility Announces Agreements to Deliver Wi-Fi Hub Solution, available at http://www.accuris-networks.com/news-and-events/in-the-news/att-roaming-hub#nav

22 Analysys Mason, Wi-Fi roaming hub providers can maximize revenue by addressing industry challenges, available at http://www.analysysmason.com/About-Us/News/Insight/Wi-Fi-roaming-providers-Aug2015/

A. While there is certainly a need to introduce greater accessibility in paying for public Wi-Fi services, it is unclear whether existing payment mechanisms (varied as they are) fail to provide sufficient accessibility between them. For example, Tata Teleservices Ltd provides wireless connectivity across over 500[23] hotspots (including the Delhi, Hyderabad, Bangalore, and Cochin airports) in the country under the brand name of 'Tata Docomo' as a freemium service: after 45 minutes of free usage, the user is required to purchase premium plans that last between 1-3 hours, using either a scratch card – which can be purchased from a counter operated by the ISP within the airport terminal – or through an online payment portal, which supports net banking and payment through credit/debit cards. In addition, the service also supports global roaming using either iPass or Boingo, and also through international cellular roaming agreements between the ISP and the user's home network operator. Between these four payment methods – scratch card, online payment and two forms of data roaming – nearly all types of users are potentially covered. Those without access to electronic payment systems can purchase a scratch card, while sophisticated users and international travelers can purchase premium access using electronic financial instruments and services.

Any proposed method to make payment for Wi-Fi less cumbersome faces two important hurdles: first, accessibility. Payment platforms such as UPI and payment wallets are accessible only by those who subscribe to them: for instance, payment through UPI presupposes that the user in question (1) possesses a smartphone; (2) operates a bank account with a bank that supports payment through UPI; (3) has the relevant mobile banking application installed; and (4) the merchant-ISP accepts payment using UPI. Similar restrictions exist as far as payment wallets are concerned. Second, supporting diverse payment methods. Given the number of payment wallets currently operating in the country, it is prohibitive (both economically, and logistically) to require ISPs/hub operators to accept payment using all of them, and arguably anti-competitive to require ISPs/hub operators to accept payment only through a select few.

23 See Tata Docomo, Wi-Fi Overview, available at https://www.tatadocomo.com/en-in/internet-wifi

As such, any proposed mandatory minimum regulations may be directed towards ensuring that ISPs/hub operators and payment gateways provide at the very least, both physical and electronic (including net banking, and pre-paid instrument based) payment mechanisms for the procurement of public Wi-Fi services. These regulations may be issued by the Reserve Bank of India pursuant to Section 10 of the Payment and Settlement Systems Act, 2007 read with the Payment and Settlement Systems Regulations, 2008. As with existing electronic payment systems, the payment platform would operate as an intermediary and would remit the amount debited from the user's bank account to the ISP/hub operator to complete a successful transaction, subject to RBI regulations applicable to financial intermediaries as well as the Information Technology (Intermediaries Guidelines) Rules, 2011 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.

QUESTION 12

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

A. Local hosting of data is required to reduce data transfer costs, assure access to important data (particularly in case of internet outages) and ensure security of data. In the current commercial context these are the basic advantages of local level hosting over cloud hosting.[24] However, when idea of local level hosting is looked at from the perspective of reducing the cost of access for consumers and the same is qualified by the idea of 'data of community interest', the following infrastructural and policy issues arise:

1. What is the cost involved in hosting data at the local level? And how to reduce the cost of local hosting?
2. How to determine what data is of community interest?
3. What are the other issues that may arise out of a local hosting policy? (Fundamentally against the principles of net neutrality)

24 Available at http://www.affinitytechpartners.com/3n1blog/2016/1/27/thinking-of-ditching-the-local-server-3-reasons-to-pause.

In the case of the proposed setup (Proliferation of Broadband by Public Wi-Fi networks), basic costs will include server acquisition costs, setting up and housing of servers, and providing server farms with uninterrupted power supply along with back-up contingencies, maintenance cost etc. Hence, a fundamental concern in this case is whether the setting up of a server and subsequent maintenance of the same costs less than the combined cost of data transfer and cloud (external) storage of locally relevant and locally generated data. In order to determine the same, we have to firstly look at advantages and disadvantages of the two. Thereafter we can determine commercial viability of local hosting or determine measures to make local hosting commercially viable.[25]

Local level hosting

Advantages

- Data is more secure.
- Run any application without any boundaries since full control is localised.
- Faster access to files, backups..
- Local access through the actual hardware in case of a network failure.
- No need for Internet access in order to access user's files.
- Problems caused by internet outages are largely decreased.

Disadvantages

- Initial capital is very high compared to cloud services.
- Maintenance costs might be high.
- IT support will be required for the maintenance of the hardware and software. (requirement of manpower)
- Delivering such infrastructure to remote, inaccessible locations.
- Limited space for data storage.

25 Available at http://www.ibs.com.cy/assets/mainmenu/111/editor/Local%20server%20VS%20Cloud%20server-what%20I%20have%20to%20choose.pdf.

Cloud hosting or hosting on the internet

Advantages

- Stable monthly costs without any initial capital.
- Limitless expansion of your servers based on your needs.
- Savings on maintenance costs.
- Access to your data from anywhere without any additional cost.
- Pay as you grow schemes which lead to cost savings in the long run.

Disadvantages

- Not compatible with every application.
- Data is stored in an external third party data centre.
- Very difficult to change cloud service providers.
- Accessing to your data might be slow since it is based on your Internet connection and prone to failure in the case of an outage.

Commercially speaking, setting up local infrastructure requires large sums of capital and maintenance of such servers, in geographically far-off places will also require large investments. This large initial investment overrides the long term benefit that may arise out of fast and unrestricted access to the internet, security of data, reduced cost of access etc.

Under such circumstances, where initial cost is high but the service pays over time, incentives have to be provided at the initial stage. These incentives will encourage initial cost bearing and over time local level hosting will pay for itself because of the reduced costs and subsequently service will become cheaper over time. Initial incentives can be provided in following three manners:

- **Government funded**[26]: Government may subsidise installation of servers at the local level. This one time cost, which is indeed substantial, can be transferred directly to the private players or a public sector unit like BSNL may be asked to undertake the establishment of basic network infrastructure. Once local servers have been set-up, management and up-

26 Efficiency of government subsidies can be seen in various cases. Few examples: http://www.forbes.com/sites/gregsatell/2013/07/02/4-government-programs-that-drive-innovation/#6a1b951b64f2

keep of the same can be transferred to private firms. These firms can in turn be subjected to regular audits in order to determine the quality of maintenance. Tax rebates for setting up local servers in identified areas may also work as an alternative to subsidising the setting up of local servers. However, a fundamental problem with this model is that the government cannot continue subsidizing the maintenance and up-keep of local servers permanently. This would be an inefficient approach. A suitable model of cost distribution to the local user base or content developers could be deployed.

- **Transferring cost to the local user base**: Cost of setting up and maintaining local servers might very well be transferred to the local user base. The best method to do this is to increase the cost of access to data stored over the local server. This method would only work if access to locally stored information is differentiated from access to information accessible from the rest of the internet. This would mean that locally stored information will have to be either accessible at a faster speed, will have to be more secure etc. or there will have to be specific information that is only accessible by using local servers. The bottom-line is that locally stored information and access to the same has to be differentiated from the rest of the information in order to make this option commercially viable.
- **Transferring the cost to content providers**: The issue of net neutrality arose because, ISPs attempted to collect revenue from large content providers, arguing that such fees would allow them to upgrade their hardware to accommodate the growing demand and better serve the end user. Some ISPs proposed another way to raise revenue, charging content providers for a "fast lane" that would give priority to their content and ensure faster delivery to the end user."[27] There is perhaps no harm in using a similar approach to finance local storage of data. A proportion of storage space can be exclusively used for storage of content of the content developer and the remaining proportion can be used for storing data of community interest. However, a fundamental problem with this approach is that it involves basic net neutrality issues and TRAI has already declared any form of preferential data transfer illegal.

27 Available at https://hbr.org/2016/06/net-neutrality-rules-will-make-winners-and-losers-out-of-businesses

Per the researcher, a hybrid of above three will be the best solution for encouraging setting up of localized servers and subsequent local storage of data. Setting up of servers in rural areas where consumers cannot bare costs can be subsidized by the government. On the other hand, the cost of such localization can be transferred directly to the consumers where they are financially capable of bearing such cost. This includes increasing the cost of access to localized content in Airports, restaurants etc., perhaps the places where luxury tax is imposed. Lastly, places where substantial number of people access certain form of content, such cost can be transferred to the content developers. This could perhaps be done in market places, taxi stands etc.

Once infrastructure is created to host data at the local level, the next big challenge is to determine what content or data is of community interest. The basic issue faced in determining the same is that different people in a community have different priorities and interests. Consequently determining community interest becomes difficult. This difficulty is further deepened by the fact that no comprehensive legal definition of community interest exists.[28] Perhaps looking at public interest may be of some help in determining community interest. Public interest may be defined as "1. The welfare or well-being of the general public; commonwealth. 2. Appeal or relevance to the general populace: a news story of public interest."[29] Considering this definition, following two methods may be adopted in order to determine community interest:

- **Public Trust Doctrine**: The Public Trust Doctrine primarily rests on the principle that certain resources have such a great importance to the people as a whole that it would be wholly unjustified to make them a subject of private ownership. The said resources being a gift of nature, they should be made freely available to everyone irrespective of the status in life. The doctrine enjoins upon the Government to protect the resources for the enjoyment of the general public rather than to permit their use for private ownership or commercial purposes.[30]

  This idea, along with the fact that an explicit arrangement is put in place that allows private owners access to the publicly owned spectrum and rights of way necessary to exploit the

28 P. Carter and J. Mayers, Division and Distribution of Community interest in defined benefit pensions (Available at http://lawschool.unm.edu/nmlr/volumes/18/1/04_carter_division.pdf)
29 Available at http://www.dictionary.com/browse/public-interest
30 Available at http://www.legalserviceindia.com/articles/ptdoc.htm; M.C. Mehta v Kamal Nath, (1997) 1 SCC 388.

technology in exchange for public access and speech rights, will ensure that the public trust doctrine is applied to enable the proliferation of broadband by Public Wi-Fi.[31] This is due to the fact that information stored locally is simply an extension of the larger internet and hence is a public utility.[32] Further, faster and secure access is being given to certain information because of it being important for the public or community interest.

Hence, keeping the above two principles in mind, the power to determine what information should be available on local servers should be vested with the government or any other body accountable and answerable to the government, and by extension civil society. Government may subsequently designate information of public importance and depending on the same determine the nature of information that is to be stored locally.[33]

- **Local community usage patterns**: Local communities may be allowed to determine the nature of information stored on the local server. This may be done by identifying local data usage patterns. Hence, information accessed most frequently by a community may be identified and stored locally. Such information in turn may be collected by identifying the internet usage pattern of the relevant local community.[34] This will not only ensure cheap access to such information but will also ensure reliability of access considering the unreliable state of wire-based broadband infrastructure. However, the basic drawback of this approach is that a community may not store data which is objectively important for it. Hence, this method should only be adopted after due deliberation and alongside behaviour tracing algorithms which balanced variables that are relevant for communities but seldom considered.
- **Hybrid approach**: This might very well be the best approach. This approach requires the government to determine the usage of a proportion of locally available space of the server and the remaining space may be used for storage of information depending on the local community's usage pattern.[35]

31 Available at http://theconversation.com/private-networks-and-public-speech-net-neutrality-in-context-37261

32 Internet was held to be a public utility in U.S.A's federal communication's ruling with respect to net neutrality. Available at http://www.nytimes.com/2015/02/27/technology/net-neutrality-fcc-vote-internet-utility.html?_r=0; Telecom Regulatory Authority of India held something on similar grounds.

33 This may include local weather forecast, information related to agriculture etc.

34 W. Aiello et al, Analysis of Communities of Interest in Data Networks, AT&T Labs-Research.

35 Researcher recommends this approach.

Despite of all these infrastructure and policy considerations, saving and granting faster and cheaper access to select content is against the core principles of net neutrality. Telecom Regulatory Authority of India's ruling dated February 8, 2016, rules against such an approach. However, regulation 6[36]may be used by the authority to relax norms in this case. Further, if the above mentioned guidelines with respect to determining nature of data of community interest are considered, relaxations can be granted considering that it is the government and the local community that discriminates between data, and not the ISPs or the content developers.

QUESTION 13

Any other issues related to the matter of consultation.

Privacy and security issues involved in proliferation of Broadband through Wi-Fi

A. While using Wi-Fi, devices and communications through them are open to anyone else using that same network. An unprotected device on public Wi-Fi may result in hackers accessing crucial personal information in seconds. Such information extends from simple information like a user's data usage rate to something as crucial as personally identifiable information or information related to an individual's financial transactions.[37]Thus the following privacy issues arise specifically in case of public Wi-Fi networks[38]:

- To use services, web sites often require the user to provide personal data such as his name, age, PIN code, or personal preferences. Many sites share this information with advertisers and other third parties. Additionally, as a recent study found, many services transmit such personal information without encryption (i.e., "in the clear").[39] A majority of the large Web-based email services, for example, encrypt the login process, but not the contents of

36 PROHIBITION OF DISCRIMINATORY TARIFFS FOR DATA SERVICES REGULATIONS, 2016.
37 Available at http://www.forbes.com/sites/amadoudiallo/2014/03/04/hackers-love-public-wi-fi-but-you-can-make-it-safe/#4c7e13ba2476
38 P. Klasnaj et al, "When I am on Wi-Fi, I am Fearless:" PRIVACY Concerns & Practices in Everyday Wi-Fi Use, Available at https://djw.cs.washington.edu/papers/wifi-CHI09.pdf.
39 Jung, J., Sheth, A., Greenstein, B., Wetherall, D., Maganis, G. and Kohno, T. Privacy oracle: A system for finding application leaks using black-box differential testing. In Proc. CCS 2008, ACM Press, (2008).

email messages. Anyone along the path between the user and the service's data centre could intercept this information, opening users to privacy and security risks.[40]

- The broadcast nature of Wi-Fi means that anyone within range of the network can receive and potentially read transmissions intended for any other device on the network. Transmissions of unencrypted personal information becomes visible to anyone within range of the network, making it much easier to track users, aggregate information over time and possibly engage in identity theft.[41]
- Since anyone can set up a Wi-Fi network and name it accordingly, this raises the possibility of malicious access points spoofing legitimate services that can capture all transmissions from unsuspecting users who connect to them.
- Much of the research shows that users don't understand that threats over W-Fi networks are real and hence do not take appropriate measures to protect against them. Hence, expecting cautious behaviour from users of public Wi-Fi networks is not practical.
- The idea of internet of things is taking shape. Many of the day to day devices are now connected to the internet and send data about their environment over the internet. If such data leaks in the process of transmission over the public Wi-Fi network, will result in grave violation of privacy of an individual.[42]

Combining these factors—accessing online services over Wi-Fi— the risk is magnified. There is a clear opportunity for technologies to be developed to help users mitigate these threats. Two existing research trajectories hold particular promise for future work: (1) develop tools that help improve users' awareness of these threats, and perhaps even give them control over preventing certain types of data from being sent unencrypted or to unauthorised parties, and (2) develop infrastructural solutions that improve Wi-Fi protocols and devices so as to eliminate the risks of

40 In the context of India, section 43A Information technology (Amendment) Act, 2008, defines civil liability for loss of PII, but does not define PII. The PII is defined under the Information Technology Rules, 2011. These rules also define a list of different types of information that either individually or in group constitute personally identifiable information. As per section 43A, if any information of the nature of PII is divulges and wrongful loss is caused to an individual due to the same, such an individual is eligible for compensation. Further the section also states that such liability is imposed when the body corporate is negligent in implementing and maintaining reasonable security practice and procedure.

41 White paper 2014, The hidden dangers of Public Wi-Fi network, Available at http://www.privatewifi.com/wp-content/uploads/2015/01/PWF_whitepaper_v6.pdf.

42 K. Rose et al, The Internet of Things: An overview (October 2015, Available at http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf).

intercepting and eavesdropping on Wi-Fi communications. As per the researcher, the following policy measures can be taken in order to secure public Wi-Fi networks for users:

- **Standard Wi-Fi security** mechanisms such as WEP and WPA must be mandatorily installed on all public Wi-Fi networks.
- **Display of standard warning message**: Display of standard message asking users to be aware of possible privacy and security threats over a Wi-Fi network may be made mandatory for Wi-Fi service providers. Such messages can include a suggestion of possible solutions like using VPNs, abstaining from sharing personal files and information over Public Wi-Fi networks etc.
- **Display of certification mark**: Security verified networks should display certificatory marks (as done in the case of celebrity verified Twitter and Facebook accounts) next to them. This will help prevent impersonation and hence enhance data security.
- **End-User Awareness Tools**: Based on above mentioned security and privacy risks one effective way to improve awareness about Wi-Fi risks is to show users how their own data is being broadcasted as they use Wi-Fi. Mirroring this type of information back to the user as they use Wi-Fi could be an effective strategy for making them more aware about certain threats and for motivating privacy- and security-conscious behaviour. Work by Kowitz & Cranor, [43] suggests a tool that would provide feedback to users about their unencrypted communications and give them some control over what is and is not sent 'in the clear'. However, a drawback of this tool is that over-attention to privacy and security threats can lead to overly restrictive use of technology even when risks are low and consequently spoil user experience over public Wi-Fi networks.
- **Infrastructural Solutions**: Networking researchers are actively exploring technical solutions that could improve the security of 802.11 protocols. Proposals such as SlyFi[44] aim to eliminate all unencrypted communication, obfuscating even the process of network discovery and association as well as routing and network management messages. This will considerably mitigate privacy and security risks currently associated with Wi-Fi use. Major

43 B. Kowitz and L. Cranor, Peripheral privacy notifications for wireless networks, Proc. WPES '05, ACM Press, (2005).
44 B. Greenstein et al, Improving wireless privacy with an identifier-free link layer protocol, Proc. MobiSys '08, (2008).

drawback of infrastructural solutions is that in order to be effective, they need both to be incorporated into wireless standards and to become widely deployed. With thousands of Wi-Fi networks in existence, it will likely be years before infrastructural solutions can truly remedy the current state of Wi-Fi security.

Considering the fact that less than half of world's Wi-Fi networks employ currently available security solutions, the deployment of such infrastructural improvements will be slow.[45] The researcher believes that what is needed in the interim is a better understanding of how end users understand and deal with Wi-Fi privacy and security threats, so that solutions, such as the aforementioned end-user awareness tools can be developed. These tools can subsequently help individuals become more informed users of Wi-Fi networks today and in the near future.

Lastly, certain policy and legal measures can also help secure personally identifiable and financially relevant information. Currently Indian law strictly punishes any form of data loss due to non-maintenance or implementing reasonable security measures by a body corporate. Under section 43A of the Information Technology Act, a body corporate can be subjected to liability for loss of information where it results in wrongful gain or loss to an individual. Further, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, made under section 43 A of Information Technology Act, 2000, comprehensively defines personally identifiable information and sensitive information. These provisions may be used to safeguard users against privacy violation over a certified public Wi-Fi network (because the law can only be applied to body corporate). However, basic problem with Indian law is that it would be difficult to hold the perpetrator liable for loss of sensitive information if such loss is not over a certified network. This is because Indian law is only applicable to a body corporate as per section 43A.

Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), may be of some help in protecting privacy and other sensitive information.[46] These regulations

45 Available at http://wigle.net.

46 Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG& toc=OJ:L:2016:119:TOC.

take a user centric approach. Under these rules, rather than nature of the violation of privacy being material, the fact that an individual's privacy was violated is material. In fact these rules go onto declare privacy as a fundamental right.[47] These rules further provide for a criteria of lawfully processing personal data in terms of use of the data for advertising and other commercial usage. Including privacy protection rules of this nature in the Indian jurisdiction may help in protecting privacy and other forms of sensitive information of public Wi-Fi networks.

Researcher is of the opinion that no one tool for protection of privacy is either better than another or conclusively effective to operate in a standalone manner. In order to protect privacy and other forms of sensitive information on Public Wi-Fi networks, the technology has to be improved, users have to be educated about cautious use of public Wi-Fi networks and implementation of the above two has to be backed by strong laws.

Balancing proliferation with net neutrality

Net neutrality is the principle that Internet service providers should enable access to all content and applications regardless of the source, and without favouring or blocking particular products or websites. The principle objective of net neutrality is that "all the Internet traffic has to be treated equally without any discrimination"; but this has had different interpretations in various contexts. The arrangement is generally that private owners can access the publicly owned spectrum and rights of way necessary to exploit the technology is exchanged for public access and speech rights. Similarly, the telephone company monopoly's use of public rights of way came with common carrier non-discrimination obligations. The broadcaster's receipt of the right of exclusive use of a coveted radio spectrum license came with public trustee obligations; and a cable operator's essentially exclusive local franchise came with obligations to provide public, educational and government access channels for free. Except under very limited circumstances (violation of criminal law), the telephone company could not deny service based on content. And, while the broadcaster's programming choices were largely insulated from government oversight, the broadcaster was still responsible for providing public access to news, public affairs and political

47 Please note that as per Supreme Court's ruling in Unni Krishnan v. State of A.P., Right to privacy is also a fundamental right under extended interpretation of Article 21 of the Constitution of India.

speech. Finally, the cable operator could exercise substantial editorial control over most channels, but larger cable systems had to set aside channel capacity for the public.[48]

Considering the above principles of net neutrality, proliferation of broadband by public Wi-Fi networks will basically raise two net neutrality issues:

- Localization of certain data for cheaper and faster accessibility inherently violates the basic principles on net neutrality. This is because in a non-discriminatory internet framework all the traffic has to be treated equally without any discrimination. However, in this approach specific nature of data is being given priority over the rest of the data.
- There are arguments stating that raising the required infrastructure for proliferation of broadband through public Wi-Fi networks requires substantial investment over long periods of time. Under such circumstances opening up access to entire web with a partially developed infrastructure is highly problematic. Content requiring high bandwidth, like streaming a video, may result in multiple users being unable to access internet due to reduced speed or no access to internet *et al*. Considering the fact that substantial investment cannot be raised overnight, selective content access may be used to make the access to internet a pleasing experience for the users. Overtime selective access will yield profits that can be re-invested in the development of physical infrastructure. Further, it is also argued that selective access will ensure development of freely available Wi-Fi at public places like airports, cafes etc. This is perhaps due to the fact that the investment requirements for a restricted access web or walled internet will be low and can be covered by product sales for cafes, shops etc.[49]

The researcher is of the opinion that despite all the infrastructure and policy considerations, selective access is against the core principles of net neutrality. The Telecom Regulatory Authority of India's ruling dated February 8, 2016, rules against this approach. However, regulation 6[50]may be used by the authority to relax norms in this case. Further, if the above mentioned guidelines with respect to determining what content is of community interest are considered, relaxations can

48 Available at https://hbr.org/2016/06/net-neutrality-rules-will-make-winners-and-losers-out-of-businesses

49 Available at http://www.cisco.com/c/en/us/about/government-affairs/government-policy-issues/net-neutrality.html

50 PROHIBITION OF DISCRIMINATORY TARIFFS FOR DATA SERVICES REGULATIONS, 2016.

be granted considering that it is the government and the local community that discriminates between data, and not the ISPs or the content developers. While the same might not be true in case of arguments with respect to infrastructural development requiring substantial investment, initial incentives have to be provided. Lastly, free public Wi-Fi should not be brought under the ambit of net neutrality. However, the same can be limited to only small stores and cafes, and content developers or ISPs may not be allowed to do the same.