INTERNET FREEDOM FOUNDATION

Shri Arvind Kumar
Advisor (Broadband and Policy Analysis)
Telecom Regulatory Authority of India

7 September 2016

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

Dear Sir,

Internet Freedom Foundation is a non-profit created by members of the Save The Internet movement for net neutrality. We aim to promote the rights of Internet users – freedom of speech, privacy, net neutrality and freedom to innovate.

We wholeheartedly support TRAI's vision to expand Internet access through the use of unlicensed spectrum, and we thank you for the opportunity to submit our counter-comments.

Please find our counter-comments below.

Thank you and best regards,
Aravind Ravi-Sulekha
Co-founder, Internet Freedom Foundation

A competitive ecosystem

Most of the comments show an assumption that the WiFi hotspot network our country needs will be set up and operated by incumbent telecom and internet service operators. On the contrary, if telcos had the ability and motivation to build out public WiFi infrastructure, they would have done so already: there's nothing preventing them. The fact that their submissions to this consultation ask for no substantive changes underlines this.

Instead, a vibrant WiFi hotspot ecosystem that will provide low-cost, high-speed Internet access to the majority of our citizens can only be built by harnessing the efforts and investment of the lakhs of small entrepreneurs that our country is fortunate to have.

There is a precedent for this.

Before mobile phones became ubiquitous in the country, the neighborhood PCO brought the telecommunication revolution to most Indians. Two key factors aided the proliferation of PCOs: economic viability and low regulatory burden.

Hotspots can potentially exceed the reach of PCOs by two orders of magnitude, as the economic case is even stronger. With the right regulations, a public WiFi service can be operated using cheap commodity hardware costing under Rs. 1,000 and without any human presence.

Anonymous access

The requirement to provide proof of identity for accessing the Internet is a serious impediment to providing universal access to all Indians.

This is effectively a prohibition of anonymous communication, which violates of our constitutional right to free expression, discriminates against the poor and marginalized and hinders investment into building Internet infrastructure for our vast nation. What's more, it has no discernable impact on the fight against crime and terrorism – the purported justifications.

This requirement is a relic that has no place in a world where the Internet is essential for our social and economic lives and central to our nation's democratic discourse.

KYC requirements stifle investment in and usage of public WiFi.

The economic viability of WiFi hotspots is greatly reduced by the compliance costs and the loss of business due to KYC.

Mobile OTP verification forces hotspot operators to buy and configure specialized hardware rather than using cheap home routers. The running costs of sending OTP messages will also be prohibitively high compared to data costs that are low and falling rapidly. ID verification imposes even higher costs by forcing hotspots to be manned by staff to collect documents.

These costs will make public WiFi much more expensive than mobile data, and therefore economically unviable.

The cumbersome, manual KYC process will also greatly reduce the market size for WiFi hotspots by excluding casual internet use. A majority of Internet usage sessions are initiated when users *receive* messages, emails, VoIP calls, notifications etc. – these would only happen if the user were already connected to the Internet. This is possible only with automated, device-negotiated authentication with known SSIDs – which is not possible with manual KYC.

The market size is also reduced by excluding people without a mobile connection – including tourists and low-income and rural families.

Anonymous communication is a fundamental human right.

The UN Special Rapporteur on Human Rights[1] has stated that the right to remain anonymous while communicating over the Internet is an intrinsic part of the right to Freedom of Expression. The ability to communicate anonymously serves an important need – both for individuals and, by enabling whistleblowers and journalists exposing wrongdoing, for society at large.[2]

Mandatory ID for accessing the Internet is unreasonable and contrary to the right to free expression as enshrined in our constitution and in the UN declaration of human rights. It is also inconsistent with established practice in democratic nations including India, which have historically respected the right to anonymity in communication through post, telegram and public telephone.

Prohibiting anonymity is ineffective in fighting crime and terrorism.

Regulations prohibiting open WiFi hotspots were a hasty and poorly considered reaction to bomb blasts in Ahmedabad in 2008, when the perpetrators claimed responsibility over email using an unsecured WiFi access point.

This regulation ignores the fact that there are many other obvious methods that criminals and terrorists may use to access the Internet without revealing their identities through IP address – such as providing fake documents or using TOR, VPNs and proxies. All of these require less effort and technical sophistication than searching for an open WiFi hotspot, and are well within the abilities of terrorists and organized criminals.

While crime and terrorism are not recent threats in our country, we have always valued the social benefit from unhindered access to communication above the dubious benefits to law enforcement and "national security" from mandatory ID checks. Accordingly, making a call at a PCO, sending a telegram and posting a letter have always been possible without showing ID – even though criminals and terrorists occasionally abused these services. There is absolutely no reason for our approach to the Internet to be any different.

Mexico's experience with mandatory KYC for the purchase of prepaid SIM cards is instructive. After 3 years of this policy from 2009 to 2012, it was repealed after statistics showed no evidence that it aided the fight against crime. On the contrary, in Mexico and China, collection of ID documents by unregulated shopkeepers *increased* instances of crimes like identity theft and fraud committed with stolen identity data.[3]

---

[1] http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/29/32&Lang=E
[2] https://www.eff.org/deeplinks/2012/01/right-anonymity-matter-privacy
[3] http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

INTERNET FREEDOM FOUNDATION

Comments to consultation questions

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

Notwithstanding the comments submitted by telcos and their trade bodies that benefit from lack of competition from WiFi hotspots, it is clear that there are serious regulatory impediments that today hamper deployment of public WiFi. The following regulatory changes are essential for the robust growth of this infrastructure:

1. Everyone must be allowed to resell Internet access without requiring a license. The UASL must be mandatory only for businesses using licensed spectrum or right-of-way.
2. There must be no KYC requirements for such unlicensed Internet access resellers.
3. There should be sufficient availability of unlicensed spectrum.
4. There should be no regulations that forbid or compel Internet access resellers to use third-party payment aggregators such as mobile wallets and banks for charging customers.

Q5. Apart from frequency bands already recommended by TRAI to DoT, are there additional bands which need to be de-licensed in order to expedite the penetration of broadband using Wi-Fi technology? Please provide international examples, if any, in support of your answer.

We agree with the various comments that suggest maximizing the amount and increasing the power limits of unlicensed spectrum, such as the 5GHz, 24GHz, 60GHz and 71-76/81-86GHz bands. We also support delicensing of TV whitespace.

Q2, Q3, Q4 and Q6 – Q12:

We share TRAI's vision of an economically viable, interoperable network of WiFi hotspots owned and operated by lakhs of small entrepreneurs with the seamless authentication and intelligent edge caching as described.

However TRAI must first *permit* such a service to be offered, before taking any regulatory measures to encourage specific attributes within that service. We believe that a competitive, deregulated WiFi hotspot ecosystem, market forces alone will likely be sufficient bring these and other consumer-friendly features into existence.

It is very premature to prescribe a particular business model or technology to achieve these aims.

It is certainly possible that WiFi Passpoint for authentication, UPI for payments, etc. will emerge as the standard. However, the market should be allowed to experiment with different models and arrive at the best solution.