INTERNET FREEDOM FOUNDATION

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

9th December, 2016

Response to the Consultation Note on Model for Nationwide Interoperable and Scalable Public Wi-Fi Networks

Dear Sir,

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

We would like to note with disappointment that our recommendations in our counter-comments to the Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks have not been accounted for so far in the consultative process. We hope that you look at our recommendations regarding KYC norms and anonymous access, which we'll reiterate in this response.

We would like to point you to our blog post that provides some general comments on this consultation note, and hope that our concerns are addressed in the ongoing consultative process.

Please find our responses to the Consultation Note below.

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

INTERNET FREEDOM FOUNDATION

Responses to consultation questions

Q1) Will the architecture suggested in the consultation note for creating unified authentication and payment infrastructure enable a nationwide standard for authentication and payment interoperability?

Most certainly not.

Technical standards are not created by a regulatory body, but by technical bodies such as IEEE, IETF, W3C, ECMA etc. Subject matter experts who are usually the highest technical authorities in the field act as editors, and the process takes multiple months or years, with widespread and open participation from industry practitioners, going through numerous versions of a detailed draft.

Even this rigorous process have often resulted in technical standards with serious flaws that hindered the chance for industry adoption. As a result, most software standards processes now proposed by IETF and W3C actually rely on industry deploying the technology in the field in parallel with the standard drafting process. This process was used, for example, in the IETF standards process for HTTP 2.0 and WebSockets, the W3C process for HTML5, CSS3 and the ECMA process for JavaScript.

For example, a small part of what TRAI proposes is an authentication system that greatly exceeds the scope of the existing authentication protocols like OpenID, OAuth and SAML. These protocols were drafted by technical experts through an open deliberative process, but nevertheless failed to live up to the original promise of universal deployment. A protocol designed in haste by TRAI alone is unlikely to succeed. Furthermore, the specification of a specific standard to the exclusion of others - without sufficient input or consideration of concerns raised via public consultation - can lead to grave competition and innovation related harms

INTERNET FREEDOM FOUNDATION

Q2) Would you like to suggest any alternate model?

Yes. TRAI should remove regulatory hurdles that currently prevent the deployment of public WiFi, and then allow the market to discover the best technical and business model.

One regulatory hurdle is the completely unreasonable "requirement" of "trusted authentication." TRAI must substantiate why it feels this is necessary. As pointed out in our earlier submission, extensive KYC norms are not effective in preventing crime, as easily available tools like VPNs, TOR, and proxies can mask Internet users' identity and location. The login related norms that have been applied to WiFi hotspots run by licensed providers and their customers has been through uncertain regulatory intervention, without open public consultation. The original February 23, 2009 direction by the Department of Telecom to ISPs made a blanket reference to alleged misuse of the internet by anti-social and anti-national elements. This direction was made without any background paper or consultation with experts or the general public. Subsequent directions and developments in the norms placed on licensees in this area were also made without public consultation in this issue. In our view, this subject itself should have been made subject to further study and inquiry by TRAI, a point which we emphasised in our original filing in the previous public Wi-Fi consultation paper.

KYC norms only serve to make WiFi hotspots more expensive and a less attractive investment for entrepreneurs. Economic and regulatory commentary has already critiqued the costs of how KYC norms are being implemented in India without resulting benefits to our security.[1] The non-existent gain in security is not a fair tradeoff for a system that is difficult to implement and restricts the right of Internet users to be anonymous.

[1] *See e.g.*, Ajay Shah, Firstpost, May 17, 2012 What security? Costs of KYC outweigh the benefits ("Open wifi networks are banned in India, because they make life difficult for policemen. This is a bad tradeoff : we have sacrificed the immense gains from ubiquitous open wifi networks in return for reducing the work of policemen.")

In addition, during the present demonetization period, we have seen credible reports of rampant identity theft used to launder black money[2]. All these crimes were enabled by various unnecessary and privacy-invading KYC requirements, for example for buying prepaid SIM cards. These "authentication" requirements merely place with untrusted third parties a large quantum of personal information that can be used for stealing identities. It is likely that KYC requirements have caused more crimes than they have prevented – a fact cited by Mexican authorities while repealing their 3-year experiment with KYC for prepaid SIM cards. Such identity verification regimes and data retention platforms have proved to be cybersecurity risks; the Real Name Verification Law brought in by the Korean Communications Commission was struck down by that country's constitutional court on grounds related to violation of rights as well as the immense risk to cybersecurity and citizen's data caused by that database.[3]

That said, where payments are to be collected (as opposed to free hotspots), the operator will need to implement some mechanism for processing these payments, and will have to comply with whatever regulations the RBI has for the payment channel.

TRAI must not mandate any hurdles, especially on free hotspots. This would have grave unintended consequences for non-profit services and public programmes already seeking to provide greater internet access using Wi-Fi.

Q3) Can Public Wi-Fi access providers resell capacity and bandwidth to retail users? Is "light touch regulation" using methods such as "registration" instead of "licensing" preferred for them?

There is no need for either registration or licensing.

Consumers and small businesses choose to share connectivity with neighbors, guests, customers, etc. Non-profit organizations may choose to serve an

[2] Business Standard, November 14, 2016
"Demonetisation: Be careful! Someone may have already used your ID proof to exchange cash"
Retrieved on 23rd November 2016.
[3] BBC, 23 August 2012, South Korea's real-name net law is rejected by court.

INTERNET FREEDOM FOUNDATION

underprivileged community. They must be allowed to do so with no additional bureaucratic hurdles.

As with any consumer or business, they must respect all the existing laws and regulations applicable to them – including respecting transmit frequency and power limitations, respecting the privacy of their users, and ensuring that their trade practices are legal and fair.

Q4) What should be the regulatory guidelines on "unbundling" Wi-Fi at access and backhaul level?

Anyone should be able to resell or share their internet access with no licensing or registration requirements. TSPs must be forbidden to add any clause in the ToS of any service that they provide under the UASL that would have the effect of preventing or hindering such resale. This would be a logical extension of previous policy decisions and regulatory updates which have made WiFi (for the frequencies specified in regulations) an unlicensed activity with respect to Indian telecom law.

Q5) Should reselling of bandwidth be allowed to venue owners such as shop-keepers through WiFi at premise? In such a scenario please suggest the mechanism for security compliance.

Of course. If TRAI's objective is to ensure widespread availability of WiFi, it must look at the example of other countries where public WiFi infrastructure is overwhelmingly provided by small shops.

We applaud TRAI on recognizing the fundamental incompatibility between the goal of universal internet access and the paranoid and pointless "security compliance" requirements. There is no way around this; **"security compliance" mechanisms are the fundamental reason why public WiFi density is abysmal in this country, and scrapping such requirements is an essential part of any solution.**

Proliferation of broadband through WiFi hotspots is impossible if TRAI insists on a mechanism that places undue emphasis on authentication and KYC norms.

INTERNET FREEDOM FOUNDATION

Q6) What should be the guidelines regarding sharing of costs and revenue across all entities in the public Wi-Fi value chain? Is regulatory intervention required or should it be left to forbearance and individual contracting?

TRAI must allow the free market to determine prices and revenue splits, subject to vigilance to ensure that the licensed oligopoly of TSPs do not engage in unfair business practices to harm independent hotspot operators. In such scenarios, TRAI should aim to identify and prohibit the unfair business practice. Price controls should be a last resort.