BOLO BHI
Advocacy - Policy - Research

MEDIA KIT

On Wednesday, the 22nd of February, the ICT R&D Fund under the Ministry of Information Technology (MoIT), announced through newspapers and their website a Request For Proposal (RFP) for national “URL filtering and blocking system”. [http://ictrdf.org.pk/RFP-%20URL%20Filtering%20&%20Blocking.pdf]

The RFP requires that: “Each [filtering] box should be able to handle a block list of up to 50 million URLs (concurrent unidirectional filtering capacity) with processing delay of not more than 1 milliseconds.” This will allow the state to subsidise a comprehensive automated censorship regime.

The ICT RnD fund that will be funding this initiative is an arm of the Pakistani Ministry of Information Technology. The fund was created in 2007 by the Ministry to take a certain percentage of revenue from telecommunications companies and allocate it for scholarships in IT education and research and development of information and communication technologies. Therefore, all grant funding for this national censorship project comes from domestic ISPs, mobile carriers, and telephone companies. However, the decision-making process by which it chooses projects and beneficiaries or grants has not been described anywhere on their website, showing a lack of transparency. Owing to the blanket nature of this ban, we issued a press release demanding transparency on the proposal.To elaborate

- The reason behind the decision
- If stakeholders were consulted before the proposal
- If implications, of the ban on various sectors, were taken into account. [http://bolobhi.org/press-release-public-statements/2222012-2/]

In Pakistan, only around 20 million out of 187 million people have access to the Internet. Despite limited access the Internet has brought positive benefits to Pakistan through economic growth, education, entrepreneurship and cultural sharing. The ICT R&D Fund was developed to further the use of ICTs and promote research in the field. It has been involved in doing that actively and therefore an announcement that is contrary to the progress and development of ICT's from the same organization comes as a shock.

FAQs:

What has happened?

The ICT R&D fund, under the ICT Ministry issued a request for proposals for a National Filtering & Blocking System on February 22, 2012. It asks applicants to submit proposals to the fund by 3pm on March 02, 2012. This was later changed to 16th March, 2012.

Who cares?

This project asks for a proposal for technology that can review 50 million website links in less than a second. Think of this as Pakistan’s very own Big Brother system, it would be a similar technology to what China government uses and is commonly known as the great firewall of China. We as rights advocates care about this initiative, because it will not only affect Internet freedom but also have economic implications. [to look at the campaign updates so far, scroll down to the Campaign Timeline]

Why does the government of Pakistan need this blocking system? What are their concerns?

The government statement suggests that the URL blocking and filtering system is required to filter out 'objectionable' content. The term hasn't been defined but past statements suggest they wish to block out pornographic, blasphemous content and content that could harm 'national security'. There's been no explanation/definition of 'national security. Due to the vagueness of the issue such a system is prone to rampant abuse.

What does National Level URL Filtering and Blocking System mean for a layman?

It means that content will be blocked on URL level. This is one of the most effective methods of blocking content, making it harder for mirror websites. It means that the government has the authority to block access to certain websites completely. In this particular instance, in the absence of legislation, it means that your website or website you use actively could be blocked without citing reasons, without providing a method to complaint, reverse wrongful block and with no time frame or contact person to approach in case of wrongful block.

This could affect business websites, research, mainstream media websites, and this will also be carried out without informing the site administrator. Violation of fundamental rights.

How can it affect an ordinary internet user?

- **Speed:** It would slow down your Internet speed.
- **Security & Privacy:** It would permit authorities to sniff into your conversations. Blanket surveillance.
- **Academic:** academic paralysis, with a rigorous filtering system, the web sphere will be limited hence it would mean less content accessible for carrying out research (you could cite example of UAE where in trying to censor porn, students could no longer access research papers on breast cancer).
- **Social networks** will not only be prone to surveillance but could be blocked just because another user has put up content that authorities consider 'objectionable’.

How does it affect various institutions:
Academia

- Academic Paralysis, limiting the scope of the Internet hence limiting research material. (In UAE while banning porn, authorities also filtered out links containing word ‘breasts’, making students unable to access research papers on breast cancer, etc).
- Censoring political figures, news or subjects to curtail political dissent would practically remove figures from history. Unfortunately our textbooks are no saviors either.
- If a college/university website is blocked, it would have major implications for students, who might be unable to apply for admissions e.g: Many university/college websites have student forums, while there are rules for the forum they are most likely to be different than rules set up by our government.

Businesses:

- Economic loses due to wrongful banning. In the absence of legislation there are no methods or rules to reverse, unspecified duration of ban and there are no legal rights given to individual businesses in case that happens (Eg: P@sha innovation fund grantee who registered a website hometownshoes.com, learnt that PTA has banned it, Jehan Ara, the President of P@sha, was able to approach the authorities and it took them ten days to reverse it. Apparently all sites containing term ‘shoes’ were banned.]

- Barrier to the flow of information: Businesses need to be able to communicate on demand, censorship restrictions limits such communication
- Innovation: Pakistan entrepreneurs need to have the scope to research and test wide number of ideas, restricting content or monitoring of their activity severely limits the ability of entrepreneurs.

Public discourse:

- During the 2007 emergency imposed by Musharraf, the media crack down resulted in an outpouring of information on social networks. These were actively used to mobilize people, spread information regarding police brutality on journalists and protesters and work as a news portal in the absence of mainstream media. Authorities recognize that this could be crucial hence a complete control on it would allow them to censor political dissent.
- A huge number of Baloch websites have already been blocked, and we have no reassurances or reasons to believe that a ‘flip flop’ switch for the internet will not be used to silence mainstream voices. Imagine mainstream media websites being banned under the same pretext.
- In a country where public discourse is limited, public spheres shrinking this will be damaging.

Could the government invade our email boxes, access social media passwords, and monitor our web activity?

Yes, because this method would enable them to access https sessions and issue their own certificates. Https means secure browsing, which is encrypted and not sniffable. An example to elaborate would be: using http your conversations are like a postcard readable to anyone, using https your message is in a sealed envelope and can only be opened by person it’s addressed to.

Can local IT experts and solution providers meet their requirements?

Essentially, they will need to buy the technology from international companies and then as the RFP suggest build it indigenously.

Will these measures slow down Internet speed too?
Yes.

Why is there such a strong protest against any such step? Isn't this step taken in good faith by the government? Why should we condemn and protest against this?

Our protest stems from government’s past record of abusing censorship, take for example the LHC decision to ban Facebook that extended to google, YouTube, blogs & even blackberry services were suspended. This is a democracy not a dictatorship. We vote and pay our taxes why should governments have to spend millions of dollars on filtering system? In the absence of legislation we are right in believing that the system is prone to abuse. The Parliament should legislate not ban.

Do you just want pornography/blasphemy in Pakistan?

It's not a matter of pornography/blasphemy or not, it's a matter of blanket censorship in Pakistan under the pretense of banning ‘objectionable content’.

Who will be responsible if people are killed on streets because of such content? Who will defend in the Court not to place a ban on such content and contest religious parties there?

The Internet by nature is a free space. It provides voluntary access to information and not imposition. It is a tool and like any other tool is prone to abuse. We don't believe all content should be freely available online and we seek to assist in limiting the criminal content that’s available, the key is to have a transparent regulatory process, with clear guidelines over what’s happening. Criminal content can only be governed if there is legislation or a law. In countries like Japan government, civil society and industry worked together to set up an organization to review illegal content. This was set up over a year ago and is operating successfully.

Explained below:

Technical Background:

1. The Government already has a tap on the International Fibers from the two peering points (TWA and PTCL), i.e. the two submarine cable operators in Pakistan.

2. All the traffic to/from Pakistan flows through these peering points and the two taps. The two taps go to “Government” where exactly (PTA? Military? Etc.) No one knows and no one wants to talk about it.

3. What happens with these existing taps? You can very well imagine, they can do DPI (Deep Packet Inspection) of all the traffic. What they cannot open right now are encrypted packets, such as packets by Skype, HTTPS sessions and VPN or other encrypted sessions.

4. Under the guise of blocking grey VOIP (voice over IP) traffic, etc. the various agencies (MI, ISI, IB, etc.) have already managed to get the taps and be able to look at the payload traffic (essentially peer into your traffic) be able to “assemble” your packet-stream and reconstruct your Web or Email or FTP session. This is very easy to do with the right tools, provided you have the ability to tap into the link. Currently Government uses Narus to do this. Remember the official story is that it is to curb Grey VOIP traffic that is supposedly causing loss to the national exchequer in the Million (Billions, etc.).

5. The government has been trying for a long time to tap into the VPN and encrypted
circuits. This they did with a legislation / circular by PTA to register ALL VPN circuits in the country. You can look at the current URL for more information (Virtual watchdog: Internet users banned from browsing privately for ‘security reasons’).

6. Now what remains to reign in the control is – blocking of URLs (porn? anti-state propaganda material, anti-Islam material?) All of these clauses are part and parcel of the various Data Communication Licenses that have been given to the various

operators. So the way PTA sees it – this is something long overdue.

7. Under the guise of the URL filtering, HTTPS sessions would also be tapped. In order to do this, all HTTPS sessions would be subjected to something called Man In The Middle Attacks (MITM). This basically says, you proxy the original HTTPS certificate/session (say as given by Gmail) and provides the user a locally owned Certificate (lets call this Pakistan URL Filtering Certificate) and with this, you have essentially been able to now

Looking into HTTPS (Secure) traffic:

8. This is a huge issue. With all the dissidents, anti-state activists, persons of interests, political figures, etc. The government will be able to see the HTTPS traffic and be able to identify the sources.

9. With Gmail, it currently establishes an HTTPS session and obfuscates the Source IP of the sender of the email. This is a stone in the government's shoe, they cannot "identify" where these people are, and with this HTTPS peering ability, they will be able to do this just so easily as they can do with HTTP sessions.

Concerns:

11. Any blanket privacy you had with respect to HTTPS is gone. So Internet banking secures communication, email, etc. all out of the door.

12. They will be able to capture all your User IDs and Password and specific answers to secret questions that you are suppose to

provide in order to recover access to your email accounts.

13. Anyone who is a whistle blower can be identified. Anyone who does not agree with the government can be identified. Anyone can be pressured. Think the McCarthyism - this is where we are heading. Big Brother is always watching and collecting information (personal dossiers) on its citizens. Now they can comfortably collect the "digital" information of its citizens.

14. The state should define and elaborate what it considers as anti-sate content. Is human rights violation in Baluchistan anti-state? Is illegal abduction and torture by intelligence agencies?

15. How does one challenge a wrong decision?

16. What are the repercussions of bypassing and viewing such content? Can it land you behind bars?

17. What / Where is the accountability factor in this?

18. How do we ensure privacy rights are not invaded when your conversations are accessible?

19. What about the MISUSE of the information collected? Pressure tactics, blackmail, etc

20. How does one challenge the government's writ in such an implementation, which is a clear and gross violation of your basic fundamental rights?

21. Who / Where are the definitions of what is anti-state, anti-religious, anti-moral etc? How do you agree on a consensus of

what a decision is? How do you challenge it? How do you modify it?
Currently the constitution states that ‘distribution’ of blasphemous and obscene content is illegal. However, such content available on the Internet is not ‘distributed’. The access is voluntary not imposing.

22. What about data-retention and data mining being done on this data collected?

23. What about Court-approved taps (such powers are supposed to be limited and only with a court-approved order are you able to insert taps). Most software vendors who provide such tapping software and reconstructions software for hand-off (technical term used in industry), have appropriate sections for implementing such Court-orders into the software for proper logging.

24. This LI (Lawful Intercept) is no longer lawful nor being monitored by any member of the legislative or court bodies. In fact it is hushed.
25. Such a system will give the government extra muscle to go after “activists” – “liberals” – “troublemakers” – You and I. Anyone who is a hindrance, becomes a target.

26. The proper way is to bring this out to the National Assembly, have it challenged and formulated with limited power, oversight committees, a quasi civilian (rotating) watchdog and with very restricted perimeters.

Campaign Timeline:
[If you are interested in learning more about the

Government's history of E-regulation and censorship attempts, please check timeline here http://bolobhi.org/resources/state-of-internet-in-pakistan-e-regulations-timeline/]

The timeline below enlists statement and media coverage the issue has received thus far.
Day one press release:
http://bolobhi.org/press-release-public-statements/2222012-2/
Day two press release:
http://bolobhi.org/press-release-public-statements/press-release-pakistan-censorship-blocking-firewall/

- Electronic Frontier Foundation issued a statement: https://www.eff.org/deeplinks/2012/02/not-a-hoax-pakistan-requests-proposals-national-filtering-and-blocking-system
- An online petition for national audience to demand an end to censorship (http://bolobhi.org/activities/petitions/pakistan-stop-the-firewall/)
- We issued letters to CEO's of international companies likely to apply (http://bolobhi.org/pakistan-anti-censorship-campaign-get-the-ceos-to-commit/) started online campaign and also a petition (http://bolobhi.org/activities/petitions/censorship-is-big-business-it-should-not-be/)
- Bushra Gohar raised issue with the ministry of IT and spoke to relevant.
- Business Human Rights Centre Committed to send our letter to the CEO's and petitions to the organizations directly
- Websense issued a statement saying they will not sell the technology and asked others to do the same (

http://bolobhi.org/press-release-public-statements/civil-society-thank-websense/) statement (http://community.websense.com/blogs/websense-insights/archive/2012/03/02/say-no-to-government-censorship-of-the-internet-in-pakistan.aspx?cmpid=pr)

- GNI issued a statement (http://www.globalnetworkinitiative.org/newsandevents/GNI_Statement_on_Pakistan_s_Request_for_Proposals_for_an_Internet_Filtering_and_Blocking_System.php) They are huge and have a lot of impact.
- Electronic Frontier Foundation issued a statement, lauding our efforts and asking other companies to take websense lead (https://www.eff.org/deeplinks/2012/03/filtering-software-companies-should-follow-websenses-lead)
- Human rights first issued statement (http://www.humanrightsfirst.org/2012/03/02/websense-applauded-for-response-to-pakistans-call-for-censorship-partner/)
- Reporters without borders issued a statement citing our petition and a letter to the Prime Minister and ICT RnD board (http://en.rsf.org/pakistan-government-wants-to-create-02-03-2012,41977.html)
- Cisco, Sandvine and Verizon have confirmed to us that they will not be selling the technology to our Government. Business Human Rights Resource Centre, our partners in the campaign, will be putting out a complete list of companies that have not responded and other's who have tomorrow (Wednesday 7th of March)

Media Coverage:

- New York Times: http://www.nytimes.com/2012/03/03/technology/pakistan-builds-web-wall-out-in-the-open.html?_r=1&smid=tw-nytimes&seid=auto
- Forbes: http://www.forbes.com/sites/davidthier/2012/03/02/pakistans-open-war-on-the-internet/
- TIME: http://www.time.com/time/quotes/0,26174,2108224,00.html
- Global Voices: http://globalvoicesonline.org/2012/02/28/pakistan-fighting-the-great-firewall/
- Express Tribune: http://tribune.com.pk/story/321958/the-futility-of-censorship/
- Firewall Looming: http://speakforchange.org/firewall-looming-in-pakistan/

ABOUT US

Our company mission and history

Established in 2012,even though we have been working on Internet freedom issues individually for over five years now, Bolo Bhi means ‘Speak up’, we are an organization with Focus on advocacy, policy and research. We are a team of individuals with diverse backgrounds who are passionate about the same causes. We believe it is crucial to bridge the gap between rights advocates, policy makers, media and average citizens. Bridging the gap enables collective strength and concentrated focus on the areas that require attention.

Biographies and credentials of key personnel

1. Chief Executive Officer & Spokesperson – Sana Saleem

Sana Saleem is an activist working on minority rights and internet freedom. She blogs at Global Voices, Asian Correspondent, The Guardian, Dawn and her personal blog Mystified Justice. She recently won the Best Activist Blogger award by CIO & Google at the Pakistan Blogger Awards. She can be found on Facebook and Tweets at: @sanasaleem. She can be contacted via email: sana<at>bolobhi<dot>org

2. Chief Operating Officer – Farieha Aziz

Farieha Aziz is a Karachi-based, APNS-awardwinning journalist. She has a masters in English literature from the University of Karachi. She worked with Newsline from July 2007-January 2012 and is currently teaching literature to grades 9-12. Her articles can be viewed here. She can be found on Twitter: @FariehaAziz and contacted via email: farieha<at>bolobhi<dot>org

3. Jehan Ara, Advisory Board

Jehan Ara is the President of the Pakistan Software Houses Association for IT & ITES (P@SHA). She is a motivator, an entrepreneur, a social activist and a strong propagator of extending the power and use of Information and communication

technologies beyond pure traditional business, to empower and enable communities. Her blog can be viewed here: In the line of Wire. She can be found on Twitter: @jehan_ara and contacted via email: jehan<at>bolobhi<dot>org