JINNAH INSTITUTE

# POLICY BRIEF

January 30, 2015

OPEN DEMOCRACY INITIATIVE


## In this Issue

This policy brief specifies five key challenges within the realm of internet policy and regulation in Pakistan and presents recommendations to address them.

***By** Jahanzaib Haque*

# Developing a Progressive Internet Policy for Pakistan

### Introduction

Increasing levels of internet use and accessibility have given rise to significant challenges across the world; Pakistan has not been an exception. However, the response to these challenges at the official level in Pakistan has been disappointing.

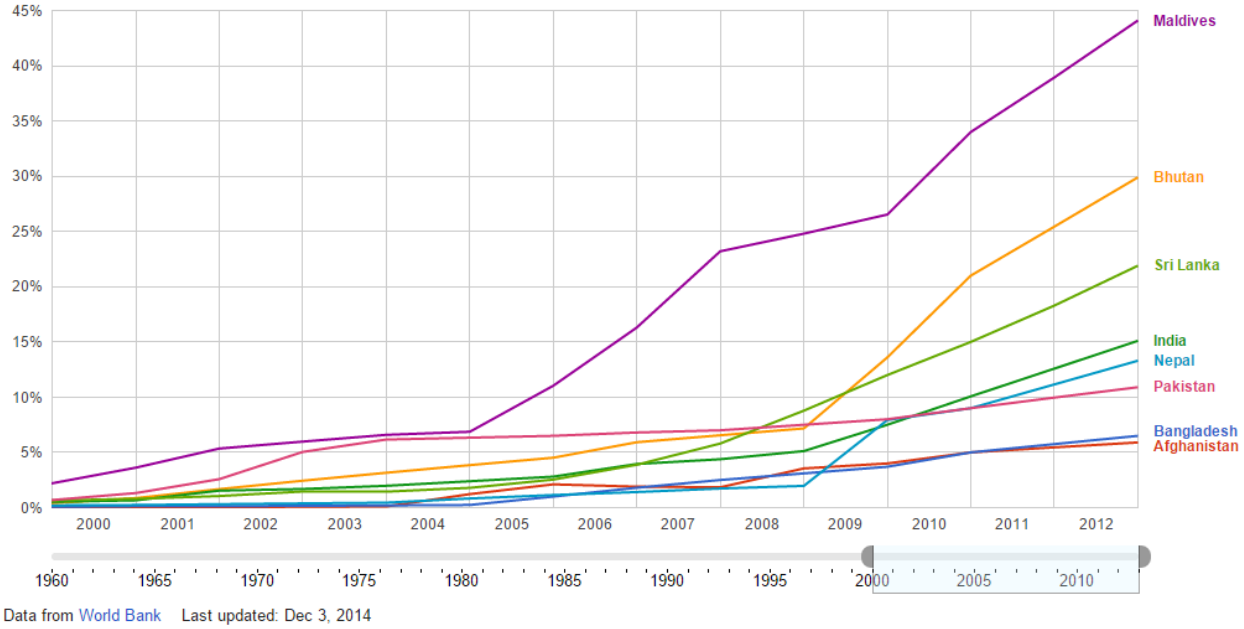
Internet policy and regulation is beset by a number of problems, including a dearth of necessary laws to govern online activity, threat of local and global monitoring, surveillance and cyber warfare, and increasing use of social media platforms to spread hate speech and terror literature.

In the absence of concrete measures to address these challenges through a progressive internet policy, there can be little that can be reaped from the opportunities that internet provides across a wide spectrum of fields. This policy brief specifies five key challenges within the realm of internet policy and regulation in Pakistan and presents recommendations to address them.

### Challenge one: Internet penetration

In the Estimates on internet access in Pakistan vary between 10 to 16 percent of the total population. This makes Pakistan one of the least connected countries in the world, ranking 142 (out of 166) on the Global ICT Index 2014, developed by the International Telecommunications Union (ITU) – the United Nations specialized agency for information and communication technologies[1]. According to ITU, Pakistan's poor ranking comes on account of stymied growth in internet access, as well as poor growth of ICT infrastructure. The ICT Index 2014 lists Pakistan's internet access growth at a low 2.95% in 2012, slightly increasing to 3.05% in 2013. The country also performed poorly on the ICT Development Index - which measures performance with regard to information and communication technology infrastructure and uptake – with growth for 2013 standing at a low 2.05%.

Internet penetration in South Asia




**Access chart**

Pakistan Telecommunications Authority (PTA), the government agency charged with the establishment, maintenance, and regulation of all telecoms had forecast in its 2011 annual report that broadband subscribers would grow rapidly to 12 million by 2015 and 19.5 million by 2020[2]. This forecast now appears misguided given the April 2014 figure of 3.6 million broadband subscribers[3]. A number of factors have hindered internet penetration in the country, as highlighted in a 2013 report titled 'Pakistan's Internet Landscape'[4]. These include:

- Internet access remains largely concentrated in urban centers, which constitute only 36% of the total population
- Political instability and state of the economy
- Power crises
- State policy, monitoring and regulation of the internet

### Recommendations:

More attention needs to be given to increase internet penetration in rural areas, which still constitute a significant share of the total population in Pakistan. The government should introduce incentives for internet service providers to expand their services to rural areas, where they are constrained by higher costs and lack of infrastructure. Business opportunities are also scarce due to lower population densities.

Mobile phone penetration carries significant potential to expand internet accessibility in rural areas. Cellular mobile teledensity stands in Pakistan stood at 76.2% of the population as of May 2014.[5]Additionally, 90 percent of Pakistanis live within areas that have mobile phone coverage.[6] With the launch of 3G and 4G services, the telecom industry is therefore well positioned to expand internet outreach to the rural population. Public-private partnerships will help in speeding up this process.

### Challenge two: Internet Censorship

Internet censorship has grown increasingly arbitrary in Pakistan. This has had a negative impact on online business and commerce and also stands in violation of the right to information and

freedom of speech as enshrined in the Constitution of Pakistan and the UN Declaration of Human Rights.

Censorship picked up pace in early 2000 and has steadily increased over the years. Online content that has been subjected to censorship can be broadly categorized as pornographic, blasphemous, or anti-state.

There are no official estimates on the number of sites blocked for internet users in the country, indicating non-transparency of the process. However, unofficial estimates from 2012 put this number between 20,000[7] to 40,000 websites[8].

One of the primary reasons for internet censorship cited by the Government is blasphemy. The most infamous ongoing case of such censorship is the ban on YouTube. The video-sharing website was blocked in September 2012 after it refused to remove a trailer of "Innocence of Muslims" - a film that insulted Islam. Other major platforms that have been blocked due to blasphemy include Facebook (2010) and Blogspot (2006).

A concerted effort has been made to block all content related to the separatist movement in Balochistan, ostensibly on the grounds of the material being "anti-state"[9]. Pornographic websites have also been widely blocked, although this has been erratic. As a result, websites on sex education and for homosexual community have also come under strict censorship[1011]. The blocking of online content is carried out through the following process:

1. All official decisions regarding censorship are made by the Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW); a body set up by the Ministry of Information Technology Information regarding the terms of reference and members of the IMCEW has still not been made public. [12]
2. Decisions made by the ICMEW are communicated to the Pakistan Telecommunication Authority (PTA), which ensures implementation through a number of measures, including:

- Notifications to ISPs regarding blocking of specified content. Failure to oblige can lead to suspension of licenses.
- Using filters set up at the Pakistan Internet Exchange, a central body which allows for effective blocking and surveillance[13]
- Using filtering software Netsweeper[14] that categorizes billions of URLs to allow for mass censorship[15]
- Agreements with online companies that allow for blocking of content. For example, the Government has a working deal with Facebook; however, details of this deal are not publicly available[16].

**Recommendations:**

Lack of transparency in the process of internet censorship has made the system vulnerable to misuse at the official level, whereby only select information may be allowed on the internet. The current system makes it impossible to identify the exact nature of blocked or censored content.

There should be internet specific laws to govern censorship and blocking of online content. More importantly, these laws should be pro-democracy and pro-people and can be derived from laws in countries where both democratic processes and internet usage are well-established.

Transparency and accountability should also be ensured in the working of official bodies involved with internet policy and regulation. These include the Ministry of Information Technology, IMCEW, Pakistan Telecommunication Authority, and the Cybercrime Wing of FIA. Basic measures such as regular updates and notifications of blocked websites can prove to be useful in terms of maintaining transparency and accountability, which would ensure that fundamental rights to freedom of speech and right to information are not being curbed. Such a measure would also allow

for affected individuals or parties to challenge decisions or address the problem so their website could, at a future point, be unblocked.

### Challenge three: Cybercrime

In spite of the threat that cybercrime poses in Pakistan, efforts to prevent online criminal activity have been sporadic at best. Again, in the absence of internet-specific laws, it has become increasingly problematic to determine what constitutes a criminal offense online.

The Cybercrime Wing at the FIA, created to deal with internet-related criminal activity, also remains unable to prosecute in a number of cases. According to one report, misuse of technology ranges from hacking of websites to outright forgery and financial fraud. The highest reported misuse, however, is cyberstalking, accounting for over 80% of internet related complaints with the FIA. Those victimized often include young women facing blackmail, harassment, and extortion[17].

The report goes on to highlight broader issues pertaining to law enforcement on the internet:

"Pakistan does not have a specific law to deal with cybercrime, particularly cyberstalking. In the absence of such a law or ordinance, the FIA cannot touch many issues. Government offices relied on the Prevention of Electronic Crimes Ordinance (PECO), 2007. When it lapsed in November, 2009, they turned to the older Electronics Transaction Ordinance (ETO), 2002, when required. Under the ETO, the highest punishment for cybercrime is a maximum of seven years in prison. According to one agency official, the FIA has been content with the conviction rate. But since there is no specific law, international internet concerns are not bound to assist in curbing incidents of cybercrime in Pakistan[18].

A new act titled Prevention of Electronic Crimes was drafted after the PECO Act lapsed in 2009. So far, the act has not been passed by the National Assembly. As such, even serious crimes such as hacking of websites, devices, and online systems have to be dealt with through the ETO, which is often inadequate for prosecution.

Efforts to curb cybercrime have been ad hoc and have often led to criminalization of free speech (discussed above). The language of laws is usually vague, with punitive action justified against loosely defined offences. For example, under the Pakistan Telecommunication (Reorganization) Act 1996, content should be regulated to ensure "national security". The Act also contains offences that are loosely defined, such as distributing "false" or "fabricated" information, sharing indecent material, and causing "mischief". Similarly, the scope of blasphemy laws has been expanded to the internet under which mass censorship has been pursued, as in the case of YouTube. "

On the other hand, the spread of hate speech and extremist literature through internet has gone largely unchecked. There has been increasing incidence of "radicalized, xenophobic, racist, and sexist discourse", along with threats targeting a range of groups including religious sects, minorities, women, and homosexuals. Hate speech against other nationalities such as Americans, Jews, Indians and Afghans has also become widespread across online forums. With particular reference to Pakistan's ongoing war against terrorism, there has been blatant use of cyberspace to overtly challenge the government and pillars of the state[19].

Due to methodological limitations, the number of recorded incidents is likely to be much lower than the actual level of criminal hate speech on the internet.

### Recommendations:

The draft of the Prevention of Electronic Crimes Bill needs to be immediately shared with relevant stakeholders and revised through consultative iterations. Once that is done, it should be

immediately brought into law. The Bill should be scrutinized in light of best practices to ensure a fair balance between freedom of expression and minimization of hate speech.

### Challenge four: Surveillance, hacking threats

The growing challenge of surveillance and hacking must be understood on two levels: local online surveillance and hacking by the state and state agencies that targets Pakistani citizens, and global surveillance and hacking carried out in Pakistan by other nation states and/or non-state actors.

In the first case, the state has worked on both technological and legislative fronts to allow for the invasion of citizens' privacy. One critical step in this direction was the establishment of the Pakistan Internet Exchange in a centralized manner that leaves the system vulnerable for monitoring the majority of Pakistan's internet traffic. As highlighted in a report by OpenNet Initiative, "PIE monitors all incoming and outgoing Internet traffic from Pakistan, as well as e-mail and keywords, and stores data for a specified amount of time. Law enforcement agencies such as the FIA can be asked by the government to conduct surveillance and monitor content".[20]

Fears of greater surveillance come from multiple media reports and research that has found evidence of spy software such as that provided by US-based Narus, Canada-based Netsweeper and the highly controversial FinFisher Command and Control Centre being used in Pakistan.[21]

Surveillance has been provided legal cover through laws such as the Fair Trial Act which allows for surveillance in a poorly defined and non-transparent manner. The Fair Trial act has been termed deeply problematic by legal experts for its potential for misuse and invasion of privacy.[22]

On the flip side, very little has been done to address the grave issue of global online surveillance and hacking that targets Pakistani institutions and citizens. This apathy exists despite whistleblower Edward Snowden's disclosure that the US spy agency NSA, in collaboration with UK's GCHQ, had been carrying out mass-scale surveillance worldwide; along with a declassified US document that states that the agency had been sanctioned to spy inside Pakistan.[23]

One concrete proposal to create a national policy on cyber security came from the Senate Committee on Defence and Defence Production. The plan included the development of new laws, the creation of a Joint Task Force for Cyber Security, the establishment of a National Computer Emergency Response Team (PKCERT) and the creation of an Inter-Services Cyber Command whose mandate would extend to coordination with the 8-member states of SAARC.[24]

### Recommendations:

The state's technological setup for online surveillance targeting Pakistani citizens needs to be analysed with the aim to ensure that misuse and abuse of the system is prevented through checks and balances. This should be done with multiple stakeholders involved (see section below) and in as transparent a manner as possible. Additionally, laws such as the Fair Trial Act need to be debated and revisited to ensure the potential for abuse is minimized.

Finally, the cyber security plan put forward by the Senate Committee on Defence and Defence Production must become a reality after being debated, refined and approved by all major stakeholders.

### Challenge five: Governance model

A large part of Pakistan's inability to adequately respond to the challenges and opportunities posed by the internet has been the result of a failure to develop a coherent governance model, both at the local and international level.

Given its globally connected, globally distributed structure, and its revolutionary impact on nearly all aspects of life, cyberspace needs governance that is multilateral, transparent and inherently democratic. Currently, there is no such model active in Pakistan. In fact, the very opposite appears to be the case.

As outlined in Pakistan's Internet Landscape report, "the government has not implemented any coherent plan to engage governments – from within the region or otherwise – the private sector, civil society or other international organizations in internet-related issues. Power to regulate and control the internet has been concentrated in the hands of politicians and the military, with little to no engagement with the business community, civil society and other stakeholders. On the international front, the government has expressed its desire to model internet governance and regulation based on China, Iran, Saudi Arabia and UAE, particularly in relation to online censorship. Such statements suggest the state aims to emulate governance from non-democratic, authoritarian setups that are directly in conflict with established human rights."[25]

**Recommendations:**

There is great need to strategically rethink the model by which the internet will be governed in the country. Further aims to centralize its governance and regulation, maintain a state of non-transparency and decision making without the inclusion of all stakeholders (particularly the IT sector, business community and civil society) will result in greater regression, stagnation and violations of basic human rights. This change needs to be recognized and implemented from the top down, beginning with lawmakers and the related state ministries and institutions.

While not an exhaustive list, major stakeholders that need to be involved include the PTA, MoIT, IMCEW, FIA National Response Centre for Cyber Crimes (NR3C), all Internet Service Providers (ISPs) individually and through the Internet Service Providers Association of Pakistan (ISPAK), PKNIC administrators who manage .pk domains, the Pakistan Software Houses Association (P@SHA) and local IT companies, and local NGOs that focus on the digital space such as Bytes for All Pakistan, Digital Rights Foundation, BoloBhi, and other citizen-led organizations.

Additionally, representatives of state should also be involved in internet governance, from lawmakers and the judiciary to the media and armed forces. Finally, focus must also be laid on engaging international stakeholders such as Google and Facebook, as well as neighboring countries, directly and through global forums on internet governance.

**Works Cited**


- *30m internet users in Pakistan, half on mobile: Report.* (2013, June 24). Retrieved December 6, 2014, from The Express Tribune: http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-onmobile-report/
- AFP. (2013, September 26). *PTA blocks website aimed at country's gay community*. Retrieved December 8, 2014, from Dawn: http://www.dawn.com/news/1045591
- Agencies. (2014, May 6). *Pakistan likely to lift ban on YouTube*. Retrieved December 8, 2014, from Daily Times: http://www.dailytimes.com.pk/national/06-May-2014/pakistan-likely-to-lift-ban-on-youtube
- *An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime*. (2013, June). Retrieved December 8, 2014, from Citizen Lab: https://citizenlab.org/2013/06/o-pakistan/
- Authority, P. T. (2011). *PTA 2011 Annual Report.* Islamabad.
- Baloch, F. (2014, November 30). *ICT ranking: Pakistan among least connected nations, stands at 142nd place.* Retrieved December 8, 2014, from The Express Tribune: http://tribune.com.pk/story/799668/ict-ranking-pakistan-among-least-connected-nations-stands-at-142nd-place/
- Chen, C. J. (2007, March 17). *Bloggers brace for blackouts over CJ*. Retrieved December 8, 2014, from Daily Times:

http://www.dailytimes.com.pk/default.asp?page=2007%5C03%5C17%5Cstory_17-3-2007_pg12_9
- Desk, W. (2012, March 20). *Pakistan blocks access to teen sex-ed site*. Retrieved December 8, 2014, from The Express Tribune: http://tribune.com.pk/story/352222/pakistan-blocks-access-to-sex-ed-site/
- Desk, W. (2013, June 20). *Pakistan government using Netsweeper for internet filtering: Report*. Retrieved December 8, 2014, from The Express Tribune: http://tribune.com.pk/story/565879/pakistan-government-using-netsweeper-for-internet-filtering-report/
- *Freedom on the net 2014: Pakistan*. (2014). Retrieved December 8, 2014, from Freedom House: https://freedomhouse.org/report/freedom-net/2014/pakistan
- Haider, M. (2014, February 16). *New cyber crimes law proposes heavy fines, jail but exempts intel agencies*. Retrieved December 8, 2014, from The News: http://www.thenews.com.pk/Todays-News-13-28608-New-cyber-crimes-law-proposes-heavy-fines-jail-but-exempts-intel-agencies
- Haque, J. (2014). *Hate Speech: A study of Pakistan's cyberspace.* Islamabad: Bytes For All Pakistan.
- Haque, J. (2013). *Pakistan's Internet Landscape Report.* Islamabad: Bytes For All Pakistan.
- Jamal Shahid, M. A. (2013, August 16). *Censoring social media: Govt caught between fans and foes*. Retrieved December 8, 2014, from Dawn: http://www.dawn.com/news/1036144
- Maqbool, A. (2010, May 19). *Pakistani court orders Facebook blocked in prophet row*. Retrieved December 8, 2014, from BBC News: http://news.bbc.co.uk/2/hi/south_asia/8691406.stm
- *Pakistan*. (2012, August 6). Retrieved December 8, 2014, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan
- *Percentage of individuals using the Internet.* (n.d.). Retrieved December 8, 2014, from International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls
- PTI. (2012, October 8). *Pakistan blocks 20,000 websites*. Retrieved December 8, 2014, from The Hindu: http://www.thehindu.com/news/international/pakistan-blocks-20000-websites/article3977440.ece
- Shahid, J. (2014, April 17). *Cyberstalking: New challenges*. Retrieved December 8, 2014, from Dawn: http://www.dawn.com/news/1078417
- *Telecom Indicators*. (2014, July). Retrieved December 8, 2014, from Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?option=com_content&task=view&id=269&Itemid=658
Yusuf, H. (2013). *Mapping Digital Media: Pakistan.* Open Society Foundations.

## References

[1](MIS 2014 Report Charts, 2014)
[2](Authority, 2011)
[3](Telecom Indicators, 2014)
[4](Haque, Pakistan's Internet Landscape Report, 2013)
[5](Telecom Indicators, 2014)
[6](The World Factbook - Pakistan, 2014)
[7](PTI, 2012)
[8](Chen, 2007)
[9](Freedom on the net 2014: Pakistan, 2014)
[10](Desk, Pakistan blocks access to teen sex-ed site, 2012)
[11](AFP, 2013)
[12](Yusuf, 2013)
[13](Pakistan, 2012)
[14](An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime, 2013)

[15](Desk, Pakistan government using Netsweeper for internet filtering: Report, 2013)
[16](Jamal Shahid, 2013)
[17](Shahid, 2014)
[18] Ibid
[19](Haque, Hate Speech: A study of Pakistan's cyberspace, 2014)
[20](Pakistan, 2012)
[21](Freedom on the net 2014: Pakistan, 2014)
[22](Imtiaz, 2012)
[23](Desk, US authorised NSA to spy on Pakistan among 193 countries, 2014)
[24](APP, 2013)
[25](Haque, Pakistan's Internet Landscape Report, 2013)