NOVEMBER 2013

PAKISTAN'S INTERNET LANDSCAPE

A Report by Bytes for All, Pakistan

Written by Jahanzaib Haque

Assistant researchers: Faria Syed,
Ferya Ilyas

www.bytesforall.pk

CONTENTS

Preface 1

Executive Summary 2

1. Pakistan Internet Laws and practices 7
1.0 Access to the Internet 7
1.1 Arbitrary blocking and filtering 8
1.1.1 Pornography 8
1.1.2 Blasphemy 9
1.1.3 Anti-state 10
1.2 Criminalizing legitimate expression 11
1.3 Imposition of intermediary liability 12
1.4 Disconnecting users from the Internet 12
1.5 Cyber-attacks 13
1.6 Surveillance and lawful intercept 14
1.7 Data protection 16
1.8 Net neutrality 16
1.9 Government engagement at the international level 16
2.0 Summary of main findings 17

2. Internet governance processes and power players 18
2.1 Relevant ministries 18
2.1.1 Pakistan Telecommunication Authority 18
2.1.2 Ministry of Information Technology 18
2.1.3 Federal Investigation Agency 18
2.2 Other relevant processes and spaces 19
2.2.1 PKNIC 19
2.2.2 Pakistan Software Houses Association 19
2.3 Powerful players 19
2.3.1 Politicians 19
2.3.2 Businesses 20
2.3.3 Military 21
2.3.4 Radical religious groups 21
2.3.5 Judiciary 22
2.4 Multi-stakeholder governance 22
2.5 Summary of main findings 22

3. Civil Society 24
3.1 Civil society active on internet issues 24
3.2 Civil society who could be activated 26
3.3 Summary of main findings 27

PREFACE

Pakistan's Internet revolution is a story of unprecedented, sometimes contentious change, as this medium of communication and information gains popularity in a largely conservative society. A country that has always struggled with freedom of speech and access to information has, at the same time, come to cherish the freedom it has found to interact, communicate and stay informed online.

With Internet penetration growing daily, there is great need for further discourse on the impact of the internet, examined in a local context, especially in relation to the state's increasing attempts to regulate and control cyberspace.

The Pakistan Internet landscape report aims to fuel that discourse, and will serve as a reference point for the ongoing debate on Pakistan's online space. The report outlines Internet control mechanisms deployed by the government, and highlights existing legislation and its application in relation to the internet. It provides a historical perspective of Internet censorship in Pakistan and the move to criminalize legitimate expression online. It also outlines the state of internet surveillance, means deployed, and the purpose and impact of such monitoring.

Lastly, the report maps the existing Internet governance infrastructure and examines different stakeholders' roles including those of government bodies, the military, businesses, politicians, the judiciary and radical religious groups, among others. The role of civil society is also examined, with a discussion on the effectiveness of citizens and organizations involved in the online space.

In capturing the past and present state of the internet in Pakistan, this report will hopefully serve as part of the roadmap to the future.

Design credit: Essa Malik

EXECUTIVE SUMMARY

In the last decade, Pakistan has seen rapid growth in information and communication technologies (ICTs), and the resultant impact these have had on society has been revolutionary, although not entirely welcomed. Ranking as the sixth most populous country in the world with over 193 million citizens, this multi-ethnic, multi-lingual yet overwhelmingly Muslim country – over 95% of the population follow Islam[1] – has struggled with the challenges posed by growing internet access.

While many economic, political and, notably, technological obstacles persist, internet penetration has seen growth to an estimated 10%[2] to 16%[3] of the population, with the country boasting 15 million mobile internet users despite a lack of 3G technology. Broadband subscriptions, comprised largely of DSL, WiMax and EvDo stand at a low 2.6 million[4] , indicating that high-speed internet is limited, even in urban areas. A large section of internet users, particularly in the rural areas, still rely on poor quality dial-up connections, or more recently, EDGE mobile connectivity, that makes most online activities difficult. In its 2011 annual report, the PTA had forecast rapid growth of broadband subscribers to 12 million by 2015 and 19.5 million by 2020[5]. However, with little strategy or planning in place, achieving such growth seems unlikely, given that broadband penetration has yet to cross 3 million in 2013.

The greatest potential for internet growth lies with cellular networks, as mobile phone teledensity in the country stands at a high 70% of the population[6] , while more than 90% of citizens live in areas that have mobile coverage[7]. A switch to 3G or even 4G mobile networks could be harnessed to provide internet access to rural areas, not only to mobile phones, but desktops, laptops and tablets as well. Unfortunately, the selling of 3G licences has been delayed since 2011 due to bureaucratic struggles and reported irregularities in tendering practices by the government[8].

To the extent that ICTs have spread, they have empowered citizens in terms of freedom of expression, access to information, citizen journalism and online activism. Internet users in Pakistan are utilizing social networks, blogs, new media, online tools and mobile applications to organize, communicate and conduct business. Unfortunately, greater freedom and internet access for citizens has been met with increased state control, and systematic surveillance and censorship of the web. Since 2007, a number of measures, both technological and legislative, have been adopted to control Pakistan's cyberspace, with justifications being derived from subjective, ill-defined terms such as 'obscenity', 'mischief', 'national security', 'terrorism' and 'anti-state' to name just a few that appear in various legal acts, ordinances and notices. The state's need to police cyberspace has led to numerous violations of fundamental rights, including freedom of speech, access to information and right to privacy.

"Greater freedom and internet access for citizens has been met with increased state control, and systematic surveillance and censorship of the web. The state's need to police cyberspace has led to numerous violations of fundamental rights, including freedom of speech, access to information and right to privacy.

The government has reportedly been aided in this pursuit by becoming a customer of technology firms such as US-based Narus[9], which allows for internet traffic monitoring and inspection, and Canada-based Netsweeper[10] which allows for the blocking and filtering of millions of sites – both processes that are facilitated through the Pakistan Internet Exchange (PIE), a core backbone set up by the government that carries a majority of Pakistan's internet traffic, allowing for easy monitoring of internet packets and installation of filters.

While blocking and filtering has been increasingly systematized in recent years, the process remains inconsistent and lacks transparency. The state offers little to no justification for the blocking of content and no established mechanisms for appealing such action, be-

1. The World Factbook - Pakistan. (2012, August 22). Retrieved September 15, 2013, from Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/pk.html
2. Percentage of individuals using the Internet. (n.d.). Retrieved October 3, 2013, from International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls
3. 30m internet users in Pakistan, half on mobile: Report. (2013, June 24). Retrieved October 3, 2013, from The Express Tribune: http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobile-report/
4. Telecom Indicators. (2013, July 10). Retrieved September 15, 2013, from Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?Itemid=599
5. Annual Report. (2011). Pakistan Telecommunications Authority. Islamabad,
6. Telecom Indicators. (2013, July 10). Retrieved September 15, 2013, from Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?Itemid=599
7. The World Factbook - Pakistan. (2012, August 22). Retrieved September 15, 2013, from Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/pk.html
8. AFP. (2013, August 7). Delays hang over Pakistan 3G lifeline. Retrieved September 15, 2013, from The Express Tribune: http://tribune.com.pk/story/587695/delays-hang-over-pakistan-3g-lifeline/
9. Freedom on the Net 2012: Pakistan. (2012). Retrieved September 15, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/2012/pakistan
10. O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime. (2013, June 20). Retrieved September 20, 2013, from Citizen Lab: https://citizenlab.org/2013/06/o-pakistan/
11. Freedom on the Net 2013. (2013). Retrieved October 6, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/freedom-net-2013
12. (2013). Freedom on the Net - Pakistan. Freedom House.

20-40,000

The reported number of blocked websites in Pakistan. The actual figures may be far higher.

yond turning to the courts. A 2013 report by Freedom House marked Pakistan's freedom status on the internet as 'not free' due to increasing obstacles to internet access, greater limits on content and a growing number of violations of user rights. Ranking Pakistan in the bottom 10 out of 60 countries examined[11] , the report cited a notable level of political censorship, blockage of social media/ICT apps and press freedom being 'not free'[12]. A 2012 report by OpenNet Initiative found Pakistan to be selectively filtering political, social content and internet tools. The study found evidence of 'substantial filtering' of content related to conflict and security. It listed transparency of the filtration process as 'medium', but highlighted low levels of consistency[13] . An earlier 2007 study by OpenNet Initiative also found that there was a greater focus on blocking blasphemous and anti-state content[14] .

The blasphemy laws, which carry the death penalty, pose the most direct challenge to the internet in Pakistan, as cases related to blasphemy such as the Facebook ban in 2010 and the YouTube ban of 2012 have shown that the pillars of the state appear to be in agreement when it comes to blocking content deemed blasphemous, although the blasphemy laws are problematic, and do not address the internet specifically *(see Section 1.1.2)*. Further pressure for blocking and filtering in relation to blasphemy comes in the form of often violent street agitation and online campaigns by right-wing, extremist and religious organizations *(see Section 2.3.4)*. These radical religious groups have rapidly expanded in the online space, operating with impunity and forming a dangerous bloc that threatens cyberspace on many levels. The use or misuse of the blasphemy laws to block parts of the internet is likely to persist until the laws are revisited, or new mechanisms are introduced for regulating the internet for blasphemous content.

Aside from blasphemy, 'obscene' or pornographic content has also been targeted, with a number of violations that remain unexplained. In 2013, torrents sites were blocked by ISPs in Pakistan[15]. In one instance, Pakistan blocked access to Scarleteen, a sex education website geared towards teenagers[16], suggesting that other educational websites and pages may be banned. In another instance, Pakistan's first website for the homosexual community queerpk.com was blocked, although the website contained no explicit or pornographic content[17].

The blocking and filtering of content that is perceived to be 'anti-state' has largely focused on stemming information about the crisis in the southern province of Balochistan, where the government has been battling an insurgency led by Baloch nationalists. The Baloch separatist movement has gained momentum in recent years, driven in part by increased access to the internet, which initially allowed Baloch nationalists[18], inside Pakistan and abroad, a largely uncensored platform to voice their dissent, demand greater autonomy and disseminate their views on the conflict. The process of blocking and filtering 'anti-state' content began in 2006, with the number of blocked Baloch websites swelling in 2009[19] and 2010, when authorities blocked The Baloch Hal, the first English language news website focused on Balochistan. By 2012, many websites, blogs and YouTube videos focused on the Balochistan conflict were blocked, although the exact number is not known due to a lack of transparency on the part of the Pakistan Telecommunication Authority[20] *(see Section 2.1.1)*.

Aside from Balochistan, there has been multiple instance of content being blocked to stem information creating a perceived negative image of politicians or the military *(see Section 1.1.3)*. Both pillars of the state cemented their control in 2006 after the formation of the Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW), a shadowy regulatory body under the MoIT, whose members include government representatives and members of security agencies *(see Section 2.1.2)*. Consequently, most arbitrary blocks and filters since 2006 have focused on benefitting both politicians and the military.

The number of blocked websites range anywhere from 20,000[21] to 40,000[22]. These reported numbers may be

11. Freedom on the Net 2013. (2013). Retrieved October 6, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/freedom-net-2013 (2013).
12. Freedom on the Net - Pakistan. Freedom House.
13. Pakistan. (2012, August 6). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan
14. Internet Filtering in Pakistan in 2006-2007. (2007). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/studies/pakistan2007
15. Online. (2013, July 24). Torrent sites and Tumblr go the YouTube way in Pakistan. Retrieved September 21, 2013, from Pakistan Today: http://www.pakistantoday.com.pk/2013/07/24/news/national/torrent-sites-and-tumblr-go-the-youtube-way-in-pakistan/
16. Pakistan blocks access to teen sex-ed site. (2012, March 20). Retrieved September 15, 2013, from The Express tribune: http://tribune.com.pk/story/352222/pakistan-blocks-access-to-sex-ed-site/
17. Abbasi, I. (2013, September 25). Pakistan blocks first gay website Queerpk.com. Retrieved September 26, 2013, from BBC News: http://www.bbc.co.uk/news/world-asia-24276142
18. Walsh, D. (2011, March 29). Pakistan's secret dirty war. Retrieved September 29, 2013, from The Guardian: http://www.theguardian.com/world/2011/mar/29/balochistan-pakistans-secret-dirty-war
19. Janjua, F. (2009, August 17). PTA goes ProPakistani - Starts Banning Anti-Pakistan Baloch Websites. Retrieved September 19, 2013, from ProPakistani: http://propakistani.pk/2009/08/17/pta-goes-propakistani-starts-banning-anti-pakistan-baloch-websites/
20. Waking up to the war in Balochistan. (2012, February 29). Retrieved September 19, 2013, from BBC News: http://www.bbc.co.uk/news/world-asia-17029159

far lower than the actual figure, given the non-transparent and inconsistent process by which content is blocked. While some blocks have been temporary in nature, others have lasted years.

In a worrying development, on October 3, 2013, the provincial government of Sindh decided to ban instant messaging and voice-over-Internet Protocol (VoIP) clients Skype, Viber, Tango and WhatsApp, for three months, claiming, "Terrorists and criminal elements are using these networks to communicate"[23] . While the ban on the apps had to be approved by the federal government, the fact that such a measure was floated drew widespread condemnation from civil society and the media who termed the move a violation of fundamental rights[24].

The only communication with internet users regarding blocking and filtering is in the form of warning messages displayed in browsers when trying to access blocked content. There are no mechanisms in place to appeal or challenge the blocks, or access a complete list of blocked sites. As a result, most citizens have turned to proxy servers, virtual private networks and tools such as Spotflux, HotSpot Shield and Tor Browser to circumvent blocks put in place. A 2013 survey on Pakistan's internet use by The Express Tribune found that over 80% of respondents used proxies or other means to bypass blocks[25]. Alexa's top sites in Pakistan still lists YouTube among the top 10 visited sites, suggesting that most, if not all citizens are aware of how to circumvent blocks[26]. Through workarounds, Pakistanis currently have access to a wide range of content. Nevertheless, the authorities push to control cyberspace has expanded beyond mere nuisance value and not only breaches constitutionally established fundamental rights of citizens, but also has a negative impact on future socioeconomic development. By examining what is blocked and what remains accessible, what is legislated against and what is not addressed, such stringent control of cyberspace appears politically motivated, geared towards hegemony over information.

The disconnection of mobile services is a disturbing new trend that could have far-reaching, negative implications, as mobile phones present the greatest potential for internet access in the country *(see Section 1.0)*. Wide-ranging disconnection has been carried out in connection to either blasphemy or terrorism *(see Section 1.4)*. The government has cited Article 148 of the Constitution as justification for the blocking of cellular services for hours across multiple cities[27]. The suspension of services has also been justified under section 54(3) of the Pakistan Telecommunication (Re-organisation) Act, titled, "National Security".

Despite Pakistan being a signatory to the UN Universal Declaration of Human Rights and having freedom of speech – with some limitations – enshrined in its Constitution, the state has increasingly criminalised legitimate expression by referring to multiple laws, such as the Pakistan Telecommunications (Re-organization) Act 1996 which gives the government broad regulatory powers. The Anti-Terrorism Act 1997 is problematic for its lack of detailed definition of what constitutes the spread of terror or sectarian hatred, particularly in relation to the internet. The act has no mention of the internet, yet is part of the PKNIC's *(see Section 2.2.1)* policy for .PK domain registration, wherein PKNIC can reject a domain registration application for being in contravention of the Anti-Terrorism Act.

The state has also systematically worked to legitimize the invasion of citizens' online privacy. In the existing legal frame work, online surveillance and lawful intercept is carried out by the PTA and multiple security agencies, which follow guidelines, set out by the government, courts and Ministry of Information Technology (MoIT). Law enforcement and intelligence agencies can conduct surveillance and monitor content either independently, or turn to the FIA and PTA for assistance.

> "Through workarounds, Pakistanis currently have access to a wide range of online content. Nevertheless, the push to control cyberspace has expanded beyond mere nuisance value and breaches constitutionally established fundamental rights of citizens.

A number of laws allow for monitoring and surveillance of the internet. The Investigation for Fair Trial Act which was passed in 2013 has given away further ground to the military in allowing online surveillance in an ill-defined, non-transparent manner. The Fair Trial Act gives security agencies the authority to collect evidence "by means of modern techniques and devices" that will be accepted in a court in cases registered un-

21. PTI. (2012, October 8). Pakistan blocks 20,000 websites. Retrieved September 21, 2013, from The Hindu: http://www.thehindu.com/news/international/pakistan-blocks-20000-websites/article3977440.ece
22. Chen, C. J. (2007, March 17). Bloggers brace for blackouts over CJ. Retrieved September 15, 2013, from Daily Times: http://www.dailytimes.com.pk/default.asp?page=2007%5C03%5C17%5Cstory_17-3-2007_pg12_9
23. Israr, F. (2013, October 4). Sindh to ban Skype, Viber, Tango. Retrieved October 6, 2013, from The Nation: http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/national/04-Oct-2013/sindh-to-ban-skype-viber-tango
24. Nasir, S. (2013, October 4). Internet activists condemn proposed ban of messaging apps. Retrieved October 6, 2013, from The Express Tribune: http://tribune.com.pk/story/613446/internet-activists-condemn-proposed-ban-of-messaging-apps/
25. Shaheryar Popalzai, J. H. (2013, August 20). Pakistan Internet Use Survey 2013. Retrieved September 27, 2013, from The Express Tribune: http://tribune.com.pk/story/591004/pakistan-internet-use-survey-2013/
26. Top sites in Pakistan. (2013). Retrieved September 20, 2013, from Alexa: http://www.alexa.com/topsites/countries/PK
27. Bikes and phones: Rehman Malik defends ban citing intelligence. (2012, November 16). Retrieved September 22, 2013, from The Express Tribune: http://tribune.com.pk/story/466731/bikes-and-phones-rehman-malik-defends-ban-citing-intelligence/

der five security-related laws[28]. The Act allows agencies to collect data from 'service providers' including telecom operators and ISPs, with failure to comply in such demands resulting in fines of up to Rs10 million and imprisonment for two years. The Act also gives service providers legal indemnity from involvement in collecting and handing over customers' private data. The actual process of obtaining a warrant is outlined: officials must submit a report to the agency's department head or a BPS-20 officer, and the approved report is then submitted to a judge. The report is then reviewed, and a warrant is issued by the judge in their chamber – a process which will not be a public record.

The Fair Trial act has been criticized by legal experts for its lack of depth, lack of clear definitions, a flawed process for obtaining warrants and an imbalance against both security agencies and citizens due to a lack of safeguards[29]. The act uses vague, ambiguous terms to describe the proof a security agency would need to obtain a warrant. The legal experts also expressed fear that the bill could be misused by security and intelligence agencies for political purposes, while also impacting fundamental rights of citizens.

In addition to the Fair Trial Act, section 54 of the Pakistan Telecommunications (Re-organization) Act 1996 allows the government to authorise any person or persons to intercept calls and messages, or to trace calls through any telecommunication system in "the interest of national security or in the apprehension of any offence"[30]. In an unprecedented move in 2011, the PTA also ordered all ISPs and mobile phone companies to ban encryption and virtual private networks (VPNs) in Pakistan as an anti-terrorism measure, based on the Monitoring & Reconciliation of International Telephone Traffic Regulations 2010[31]. In theory, the law would allow easier surveillance of unencrypted data for the government in what is tantamount to a breach of privacy. In giving security agencies such wide-ranging technological means and legislative cover to access citizens' private lives and conversations, the likelihood of misuse is high. While there is a great need for laws that deal with use of the internet in connection to illegal activities, the existing legislation and practices are flawed and open to misuse and human rights violations.

Cyber-attacks have been a part of Pakistan's online space since over a decade, and almost entirely in connection with neighbouring India *(see Section 1.5)*. Most of the reported attacks fall under 'hacktivism' i.e. political hacking to promote an ideological viewpoint. Generally, attacks have had a limited scope and time frame, consisting mostly of website defacement, denial of service attacks and a low level of sophistication. It is unclear whether they are conducted as part of state-sanctioned/funded operations, or by independent, ideologically motivated individuals. A 2004 report by the Institute for Security Technology Studies cites "possible ties between the hacker community and Pakistani intelligence services…it is quite possible that the government of Pakistan has made only a minimal investment in its cyber warfare program." [32]

There are no laws in Pakistan specific to cyber-attacks and hacking. The highly problematic Prevention of Electronic Crimes Ordinance 2007 was implemented for a brief period, containing harsh punishments related to cyber-attacks, but the ordinance lapsed in 2009. In its absence, the FIA has been registering cases under sections 36 and 37 of the 2002 Electronic Transaction Ordinance (ETO), which deal with violation of privacy information and damage to information systems, along with section 419 (Punishment for cheating by impersonation) of the Pakistan Penal Code[33]. FIA officials have said prosecuting under the ETO causes massive delays as the case grade is low, and "people often get away with the crime"[34]. Aside from the online Pak-India conflict, cyber-attacks within Pakistan are increasingly aimed at e-commerce sites and unsecure telecommunication networks[35]. Both hacktivism and attacks on online businesses pose a real threat that needs to be addressed, both legislatively and through action by the security apparatus or relevant agencies. The issue has been taken up by the Senate Committee on Defence and Defence Production, which aims to create a national policy on cyber security *(see Section 2.3.1)*.

Given the collusion between the government and the military in creating and maintaining the current state of the internet, the promise of a freer, more democratic cyberspace lies in the hands of a number of key players that would have to work towards a multi-stakeholder model of governance. ISPs have struggled with little success against the government, which held a virtual monopoly through the state-controlled PTCL till 2009. After PTCL's partial privatization and the decision to allow ISPs to buy bandwidth from other third-party

28. Investigation for Fair Trail Act. (2013, February 22). Gazette of Pakistan. Islamabad, Pakistan.
29. Imtiaz, S. (2012, October 22). Pakistan's 'patriot act'?: How fair is the new trial bill? Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/454973/pakistans-patriot-act-how-fair-is-the-new-trial-bill/
30. Pakistan Telecommunication (Re-organization) Act. (1996, October 17). The Gazette of Pakistan. Islamabad, Pakistan.
31. Asia Pacific: Free expression and law in 2011. (2012, April 5). Retrieved September 20, 2013, from Article 19: http://www.article19.org/resources.php/resource/3026/en/asia-pacific:-free-expression-and-law-in-2011
32. (2004). Cyber warfare: an analysis of the means and motivations of selected nation states. Institute for Security Technology Studies at Dartmouth College.
33. Man sent into custody for harassing girl on Facebook. (2013, September 25). Retrieved September 27, 2013, from The Express Tribune: http://tribune.com.pk/story/608681/cyber-crime-man-sent-into-custody-for-harassing-girl-on-facebook/
34. Zeeshan, O. (2011, March 24). Investigators suffering from absence of law. Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/136794/investigators-suffering-from-absence-of-law/
35. Ashraf, G. (2011, April 3). Cyber wars. Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/140431/cyber-wars/

providers[36], a certain level of independence was attained, aided by ISPAK – a single body representing the ISPs. Unfortunately, existing legislation and regulations have left ISPs unable to defend their customers' basic rights. Little effort has been made by ISPs to change the existing environment to be conducive to a more democratic and open internet.

Unfortunately, the judiciary has yet to play an active role in correcting the increasing levels of state control of the internet *(see Section 2.3.5)*. In fact, lawyers and judges have worked towards greater blocks and filters online in the past [37]. As the IT and telecommunications industry grows and more businesses and local media move online *(see Section 2.3.2)*, it is likely that the systems and legislation by which the internet is governed will come under greater scrutiny, criticism and hopefully, change.

Another progressive force is Pakistan's civil society, which is at a nascent stage online, yet has already proven itself to be capable of thwarting government plans to control the internet *(see Section 3.1)*. The online community is capable of organizing and leading protests – both online and on-ground – to push back against state control and interference. Civil society members and activists are supported by a handful of non-profits and NGOS that work specifically on internet-related issues. These organizations have aided in enhancing awareness, providing structure and actionable points to protests as well as taking direct action such as court petitions.

In the case of the national URL filtering system and the SMS word filtration plans, the ensuing social media uproar, resultant media coverage, online petitions and efforts of civil society organizations led to the PTA deciding against pursuing the projects. Notably, Bolo Bhi, a not-for-profit organization based in Pakistan worked with other groups to convince five international companies that sell surveillance, filtering and blocking systems to publicly commit not to apply for Pakistan's URL filtering project[38]. Bolo Bhi Director Sana Saleem along with bloggers Dr Awab Alvi, Faisal Kapadia and others also took the government to court against its practise of blocking websites and the plan to have a national filtering system in place. Another notable example was Bytes for All (B4A) - a human rights organization that announced it would challenge the validity of the SMS filter in court[39]; part of the immense pressure put on the PTA that eventually issued a statement, saying it was withdrawing the order[40] .

The unexplored potential of civil society is largely dependent on whether key influencers in the online space – celebrities, religious leaders and NGOs – *(see Section 3.2)* can be engaged to form a more cohesive and powerful community. The great challenge for civil society is the rising tide of online extremism, whose messages resonate with the conservative, religious majority in opposition to free, open and safe internet in Pakistan.

36. Pakistan. (2012, August 6). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan
37. LHC bans Facebook while protests continue. (2010, May 19). Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/14370/lhc-bans-facebook-till-may-31/
38. Ribeiro, J. (2012, April 2). Groups Pressure Pakistan to Stop National Internet Monitoring Plan. Retrieved September 26, 2013, from PC World: http://www.pcworld.com/article/253005/groups_pressure_pakistan_to_stop_national_internet_monitoring_plan.html
39. Moral Policing gets an Upgrade in Pakistan. (2011, November 18). Retrieved September 26, 2013, from Bytes For All: http://content.bytesforall.pk/moral_policing
40. Attaa, A. (2011, November 22). PTA Decides to Withdraw SMS Filtration Orders. Retrieved September 26, 2013, from ProPakistani: http://propakistani.pk/2011/11/22/pta-decides-to-withdraw-sms-filtration-orders/

1.PAKISTAN INTERNET LAWS AND PRACTICES

1.0 ACCESS TO THE INTERNET

Estimates of internet users in Pakistan range from 10%[41] to 16%[42] of the overall population. Online access is provided by 50 operational Internet service providers (ISPs), of which 10 provide high-speed services[43]. Broadband subscriptions, comprised largely of DSL, WiMax and EvDo stand at a low 2.6 million[44], indicating that high-speed internet is limited, even in urban areas. A large section of internet users still rely on poor quality dial-up connections, or more recently, mobile connectivity, that makes most online activities difficult. The Internet Service Providers Association of Pakistan (ISPAK) – a platform representing ISPs in the country *(see Section 2.3.2)* – cites 15 million[45] mobile internet users on the slow EDGE network, as the country has yet to shift to 3G, although a 3G policy was approved in November 2011[46].

A major part of the challenge to greater internet penetration has been the urban-rural digital divide. A majority of Pakistan's internet users are located in the urban centres, which comprise only 36% of the total population[47]. A BBC survey in 2008 found that 34% of the urban population said they had access to the internet, as compared to only 3% of the rural population[48]. The spread of the internet to rural areas has been limited due to the high cost for ISPs to provide service in areas with low population density, a lack of existing infrastructure as well as cultural barriers, low literacy and the relatively high cost of internet in the country.

Another major factor that has impacted internet access is political instability and the state of the economy. Internet penetration in Pakistan increased from 6.3% in 2005 to 15.7% in 2008[49] during a period of economic boom under the then President, General Pervez Musharraf. After a period of social and political turmoil that led to an end of Musharraf's nearly decade long rule, the change of government in 2008 was followed by a decline in economic growth – a period which also saw internet penetration slow down significantly, growing from 15.7% in 2008 to just 16.7% by 2010. The country's years-long power crisis has also directly affected internet use, as both urban and rural areas face up to 20 hours of blackouts, scheduled and unscheduled load-shedding[50].

State policy, monitoring and regulation with regards to the internet have also had an impact on internet access. In its 2011 annual report, the PTA had forecast rapid growth of broadband subscribers to 12 million by 2015 and 19.5 million by 2020[51]. However, with little strategy or planning in place, achieving such growth seems unlikely, given that broadband penetration has yet to cross 3 million. A 2013 Freedom House report cites inadequate monitoring of internet service quality by the PTA as having a negative impact on the spread of broadband internet[52].

Perhaps the greatest potential for internet growth lies with mobile networks, as mobile phone teledensity in the country stands at a high 70% of the population[53], while more than 90% of citizens live in areas that have mobile coverage[54]. Aside from immediate improvement in internet quality for smartphone users in Pakistan, a switch to 3G or even 4G mobile networks could be harnessed to provide internet access to rural areas, not only to mobile phones, but desktops, laptops and tablets as well. Unfortunately, the selling of 3G licences has been delayed since 2011 due to infighting within the PTA and reported irregularities in tendering practices by the government[55].

2.6m

Broadband subscriptions in Pakistan, comprised largely of DSL, WiMax and EvDo.

41. Percentage of individuals using the Internet. (n.d.). Retrieved October 3, 2013, from International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls
42. 30m internet users in Pakistan, half on mobile: Report. (2013, June 24). Retrieved October 3, 2013, from The Express Tribune: http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobile-report/
43. ISPAK. (2012, April 26). Retrieved September 15, 2013, from Internet Service Providers Association of Pakistan: http://www.ispak.pk/
44. Telecom Indicators. (2013, July 10). Retrieved September 15, 2013, from Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?Itemid=599
45. ISPAK. (2012, April 26). Retrieved September 15, 2013, from Internet Service Providers Association of Pakistan: http://www.ispak.pk/
46. PM okays 3G policy for telecom sector. (2011, November 24). Retrieved September 15, 2013, from Dawn.com: http://beta.dawn.com/news/675552/pm-okays-3g-policy-for-telecom-sector
47. The World Factbook - Pakistan. (2012, August 22). Retrieved September 15, 2013, from Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/pk.html
48. Internet in Pakistan. (n.d.). Retrieved September 15, 2013, from Audiencescapes: http://www.audiencescapes.org/country-profiles-pakistan-country-overview-internet-research-statistics
49. Yusuf, H. (2013). Mapping Digital Media: Pakistan. Open Society Foundations.
50. Freedom on the Net 2012: Pakistan. (2012). Retrieved September 15, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/2012/pakistan
51. Annual Report. (2011). Pakistan Telecommunications Authority. Islamabad.
52. (2013). Freedom on the Net - Pakistan. Freedom House.
53. Telecom Indicators. (2013, July 10). Retrieved September 15, 2013, from Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?Itemid=599
54. The World Factbook - Pakistan. (2012, August 22). Retrieved September 15, 2013, from Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/pk.html
55. AFP. (2013, August 7). Delays hang over Pakistan 3G lifeline. Retrieved September 15, 2013, from The Express Tribune: http://tribune.com.pk/story/587695/delays-hang-over-pakistan-3g-lifeline/

1.1 ARBITRARY BLOCKING AND FILTERING

Instances of arbitrary blocking and filtering of the online space have steadily increased since 2005. State action has been seen in a few broad categories that include content deemed pornographic, blasphemous or anti-state.

Blocking and filtering of online content is reportedly being carried out by the government using filtering software supplied by Canadian firm Netsweeper. A report by Citizen Lab, a research centre at the University of Toronto uncovered evidence that Netsweeper, which has categorized over five billion URLs, and adds approximately 10 million new URLs every day, would give the PTA sweeping powers to block and filter content[56]. Evidence of Netsweeper's use comes after the government circulated a document in 2012 seeking filtering software. "Pakistani ISPs and backbone providers have expressed their inability to block millions of undesirable websites using current manual blocking systems," the government had stated in the paper, adding that it needed a system "able to handle a block list of up to 50 million URLs"[57]. Aside from the use of Netsweeper, and filters at the Pakistan Internet Exchange, ISPs are required to carry out blocking directives issued by the PTA, or face license suspensions for failure to respond.

While there is no clear number of how many websites have been blocked in Pakistan, the use of Netsweeper, filters at PIE and the ISPs place estimates anywhere from 20,000[58] to 40,000 sites which Pakistani users are restricted from viewing[59]. These reported numbers may be far lower than the actual figure, given the non-transparent and convoluted process by which content is blocked. This includes sites blocked at the domain and subdomain level, as well as URL-specific content. The only communication with internet users regarding blocking and filtering is in the form of warning messages displayed in browsers when trying to access blocked content. The message generally warns users that the content they are trying to access has been blocked by orders of the PTA. There are no mechanisms in place to appeal or challenge the blocking of content, or access a complete list of blocked sites.

In a worrying development, on October 3, 2013, the provincial government of Sindh decided to ban instant messaging and voice-over-Internet Protocol (VoIP) clients Skype, Viber, Tango and WhatsApp, for three months, claiming, "Terrorists and criminal elements are using these networks to communicate"[60]. While the ban on the apps had to be approved by the federal government, the fact that such a measure was floated drew widespread condemnation from civil society and the media who termed the move a violation of fundamental rights[61].

"The only communication with internet users regarding blocking and filtering is in the form of warning messages displayed in browsers when trying to access blocked content. There are no mechanisms in place to appeal or challenge the blocking of content, or access a complete list of blocked sites.

As a result, most citizens have turned to proxy servers, virtual private networks and tools such as Spotflux, HotSpot Shield and Tor Browser to circumvent blocks put in place. A 2013 survey on Pakistan's internet use by The Express Tribune found that over 80% of respondents used proxies or other means to access blocked content[62]. Alexa's top 100 sites in Pakistan still lists YouTube among the top 10 visited sites, suggesting that most, if not all citizens are aware of how to circumvent blocks[63].

1.1.1 Pornography

The banning of online pornographic content began as far back as 2003, when more than 1,800 sites described as a "corrupt and evil influence" were blocked under government orders[64]. The list of blocked sites was not made publicly available. The Ministry for Information Technology (MoIT) had the ban implemented through content filters set up at the internet exchanges[65]. At the time, the government considered developing and circulate software that would allow citizens to block

56. O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime. (2013, June 20). Retrieved September 20, 2013, from Citizen Lab: https://citizenlab.org/2013/06/o-pakistan/
57. Reuters. (2013, September 18). Pakistan's internet censors seek help from Canadian company. Retrieved September 22, 2013, from Dawn: http://dawn.com/news/1043768/pakistans-internet-censors-seek-help-from-canadian-company
58. PTI. (2012, October 8). Pakistan blocks 20,000 websites. Retrieved September 21, 2013, from The Hindu: http://www.thehindu.com/news/international/pakistan-blocks-20000-websites/article3977440.ece
59. Chen, C. J. (2007, March 17). Bloggers brace for blackouts over CJ. Retrieved September 15, 2013, from Daily Times: http://www.dailytimes.com.pk/default.asp?page=2007%5C03%5C17%5Cstory_17-3-2007_pg12_9
60. Israr, F. (2013, October 4). Sindh to ban Skype, Viber, Tango. Retrieved October 6, 2013, from The Nation: http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/national/04-Oct-2013/sindh-to-ban-skype-viber-tango
61. Nasir, S. (2013, October 4). Internet activists condemn proposed ban of messaging apps. Retrieved October 6, 2013, from The Express Tribune: http://tribune.com.pk/story/613446/internet-activists-condemn-proposed-ban-of-messaging-apps/
62. Shaheryar Popalzai, J. H. (2013, August 20). Pakistan Internet Use Survey 2013. Retrieved September 27, 2013, from The Express Tribune: http://tribune.com.pk/story/591004/pakistan-internet-use-survey-2013/
63. Top sites in Pakistan. (2013). Retrieved September 20, 2013, from Alexa: http://www.alexa.com/topsites/countries/PK
64. Pakistan tackles web porn. (2003, July 3). Retrieved September 15, 2013, from BBC News: http://news.bbc.co.uk/2/hi/technology/3041022.stm
65. PTCL directed to block porno, blasphemous sites. (2003, January 29). Retrieved September 15, 2013, from Dawn: http://beta.dawn.com/news/79886/ptcl-directed-to-block-porno-blasphemous-sites

websites themselves[66].

In March 2004 the Federal Investigation Agency (FIA) ordered ISPs to block online pornography[67]. Most of these blocks were largely symbolic, as a 2007 OpenNet Initiative study found that "pornographic content was largely accessible, with only symbolic blocking of selected sites" due to the lack of a sophisticated blocking system, and a greater focus on blasphemous and anti-state content[68].

In 2011, the PTA and Supreme Court of Pakistan websites were defaced by a hacker under the alias Zombie_Ksa who demanded the PTA Chairman and Chief Justice of Pakistan order the PTA to block access to all online pornography[69]. Under pressure from the courts[70], over 1,000 pornographic sites were blocked by ISPs on orders of the PTA, and orders to block more sites were relayed on a daily basis[71]. By 2012, Parliamentary Secretary for Information Technology Nawab Liaqat Ali Khan told Parliament that the government had blocked 13,000 'obscene' websites on the internet[72].

In 2013, torrents sites were blocked by ISPs in Pakistan[73]. While no justification was provided for the blockage, reports suggested that the block was in connection to pornographic content accessible through peer-to-peer torrent networks, or the availability of pirated content[74].

While partial lists of blocked websites were obtained by local media, the complete list of 'obscene' websites has not been made publicly available, raising concerns about what content is being blocked under the broad term 'obscene' and similar vague definitions in the Pakistan Telecommunications (re-organisation) Act,1996 *(see Section 1.2)*.

In one reported instance, Pakistan blocked access to Scarleteen, a sex education website geared towards teenagers[75], suggesting that other educational websites and pages may be banned. In another instance, Pakistan's first website for the homosexual community queerpk.com was blocked, although the website contained no explicit or pornographic content[76].

1.1.2 Blasphemy

The few occasions where the state has been forthcoming about its justifications for blocking online content has been in the case of blasphemy. The Pakistan Penal Code's sections 295-A, 295-B, 295-C, 298, and 298-A are collectively referred to as the blasphemy laws, and carry the death penalty. In practice, the laws have largely been misused to target minorities. The National Commission for Justice and Peace identified that in the last 25 years, 1,058 cases of blasphemy were registered, of which 456 accused were Ahmadis, 449 were Muslims, 132 were Christians and 21 were Hindus[77], exhibiting the disproportionate use of the laws against minority groups.

In the online space, the blasphemy laws are solely applied to block content related to Islam. In 2003, the government began the process of blocking blasphemous sites[78], along with proxy sites being used to access blocked content[79]. The government's first implementation of a widespread ban came directly after the Danish cartoon controversy in 2006, where Danish and Norwegian newspapers ran caricatures depicting the prophet Muhammad (pbuh) – an act considered blasphemy in Islam. The Supreme Court of Pakistan directed the government to block all websites hosting the caricatures, while the petitioner in the case argued that the availability of such material "should have been declared as intellectual terrorism and a war of the East against the West."[80] The PTA consequently began a crackdown on blasphemous sites, which led to the block of popular blogging site blogspot.com (or blogger.com), ending access to thousands of hosted blogs in Pakistan[81]. The ban on blogspot.com lasted nearly two months.

An accidental blanket ban occurred in 2008, when the government ordered ISPs to block a URL and IP addresses of a YouTube video of Dutch lawmaker Geert Wilders that was deemed blasphemous. As the internet exchange could not perform a URL-specific block, an IP-wide block was initiated that rendered the

66. Pakistan tackles web porn. (2003, July 3). Retrieved September 15, 2013, from BBC News: http://news.bbc.co.uk/2/hi/technology/3041022.stm
67. Ali, G. (2004, March 5). FIA asks Internet Service Providers to block porno sites. Retrieved September 15, 2013, from Daily Times: http://www.dailytimes.com.pk/default.asp?page=story_5-3-2004_pg7_36
68. Internet Filtering in Pakistan in 2006-2007. (2007). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/studies/pakistan2007
69. Popalzai, S. (2011, September 27). Compromised: Official website of the SC hacked. Retrieved September 15, 2013, from The Express Tribune: http://tribune.com.pk/story/261497/hacker-defaces-supreme-court-website/
70. PPI. (2011, October 18). Obscene websites case: SHC gives 10 days to PTA for filing comments. Retrieved September 15, 2013, from The Express Tribune: http://tribune.com.pk/story/276751/obscene-websites-shc-gives-10-days-to-pta-for-filing-comments/
71. Haque, J. (2011, November 17). PTA approved: Over 1,000 porn sites blocked in Pakistan. Retrieved September 15, 2013, from The Express Tribune: http://tribune.com.pk/story/293434/pta-approved-over-1000-porn-sites-blocked-in-pakistan/
72. Government blocks 13,000 obscene websites: Official. (2012, February 9). Retrieved September 15, 2013, from The Express Tribune: http://tribune.com.pk/story/334055/government-blocks-13000-obscene-websites-official/
73. Online. (2013, July 24). Torrent sites and Tumblr go the YouTube way in Pakistan. Retrieved September 21, 2013, from Pakistan Today: http://www.pakistantoday.com.pk/2013/07/24/news/national/torrent-sites-and-tumblr-go-the-youtube-way-in-pakistan/
74. Ban on websites. (2012, June 8). Retrieved September 21, 2013, from The Express Tribune: http://tribune.com.pk/story/390782/ban-on-websites/
75. Pakistan blocks access to teen sex-ed site. (2012, March 20). Retrieved September 15, 2013, from The Express tribune: http://tribune.com.pk/story/352222/pakistan-blocks-access-to-sex-ed-site/
76. Abbasi, I. (2013, September 25). Pakistan blocks first gay website Queerpk.com. Retrieved September 26, 2013, from BBC News: http://www.bbc.co.uk/news/world-asia-24276142
77. Alvi, A. S. (2012, September 29). Abating tolerance and blasphemy laws . Retrieved September 29, 2013, from Daily Times: http://www.dailytimes.com.pk/?page=2012%5C09%5C29%5Cstory_29-9-2012_pg3_5
78. PTCL directed to block porno, blasphemous sites. (2003, January 29). Retrieved September 15, 2013, from Dawn: http://beta.dawn.com/news/79886/ptcl-directed-to-block-porno-blasphemous-sites
79. PTCL begins blocking proxy servers: Proscribed sites. (2003, July 28). Retrieved September 15, 2013, from Pakistan Press Foundation: http://www.pakistanpressfoundation.org/news-archives/23883/ptcl-begins-blocking-proxy-servers-proscribed-sites/
80. Websites blocked, PTA tells SC: Blasphemous material. (2006, March 14). Retrieved September 19, 2013, from Pakistan Press Foundation: http://www.pakistanpressfoundation.org/news-archives/31701/
81. Blogspot.com blocked again. (2006, May 10). Retrieved September 19, 2013, from Reporters Without Borders: http://archives.rsf.org/article.php3?id_article=16678

entire YouTube domain inaccessible across most parts of the globe for almost two hours[82]. The ban on YouTube was lifted by the PTA in four days after the website removed "highly profane and sacrilegious footage". It was not confirmed whether YouTube had actually removed any content[83].

The blocking of entire domains was undertaken again in 2010, when the PTA ordered ISPs to block Facebook, YouTube, and some Flickr and Wikipedia pages following the creation of a Facebook page titled "Post Drawings of the Prophet Mohammad Day". The decision came after agitation and street protests led by religious groups and citizens across Pakistan. The judiciary was actively involved in the block, as the Islamic Lawyers Association requested a court injunction to ban Facebook, leading to the site being blocked for nearly two weeks in May by order of the Lahore High Court[84]. Approximately 10,548 websites were blocked[85], while telcos also halted BlackBerry web-browsing services completely for some time[86]. The ban on Facebook was lifted after the blasphemous page was removed. At the time, MoIT officials told the court that 'senior management 'at Facebook had assured blockage of blasphemous material. The then Chief Security Officer of Facebook Joe Sullivan allegedly assured the ministry that Facebook would filter data available on the website[87]. YouTube was also unbanned, with government officials claiming specific video links would be blocked[88].

In 2012, micro-blogging site Twitter was blocked for less than a day for hosting posts promoting a competition for blasphemous drawings[89]. Later in the year, the trailer of Sam Bacile's 'Innocence of Muslims' was released on YouTube, leading to large-scale, violent street protests that left 20 dead in Pakistan and the eventual year-long blanket ban on the video-hosting site[90]. The ban on YouTube remains in place, despite the government's announcement that it is working on resolving the issue. A petition against the ban was filed by Bytes for All, which termed any filtering and blocking on internet "counter-productive and predatory"[91]. The case is being heard by the Lahore High Court.

10,548

Websites were blocked after Facebook was banned for nearly two weeks in May 2010.

Certain sites of the minority Shia and Ahmadi communities were also blocked in 2012. PTA officials stated the Ahmadi website alislam.org was blocked because Ahmadis were not allowed to propagate their religious views under the Constitution of Pakistan, while a second source said the site was blocked for hosting blasphemous content[92]. Days later, shiakilling.com – a watchdog site tracking the murder of Shias – was blocked, leading to street protests by the Shia community[93]. The website was unblocked after the then Interior Minister Rehman Malik ordered the removal of "objectionable material" from the site[94].

1.1.3 Anti-state

The blocking and filtering of content that is perceived to be 'anti-state' has largely focused on stemming information about the crisis in the southern province of Balochistan, where the government has been battling an insurgency led by Baloch nationalists[95]. The Baloch separatist movement has gained momentum in recent years, driven in part by increased access to the internet, which initially allowed Baloch nationalists a largely uncensored platform to voice their dissent, demand greater autonomy and disseminate their views on the conflict.

The process of blocking and filtering 'anti-state' content began in 2006, when the PTA issued a letter to ISPs ordering the blocking of websites publishing news and opinion on Balochistan and Baloch political autonomy. The sites were blocked on the grounds of

82. Pakistan. (2012, August 6). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan
83. AFP. (2008, February 27). Pakistan lifts YouTube ban. Retrieved September 19, 2013, from ABC News: http://www.abc.net.au/news/2008-02-27/pakistan-lifts-youtube-ban/1054918?section=world
84. LHC bans Facebook while protests continue. (2010, May 19). Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/14370/lhc-bans-facebook-till-may-31/
85. LHC asked to order Facebook owners' arrest. (2010, July 10). Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/26886/lhc-asked-to-order-facebook-owners-arrest/
86. Attaa, A. (2010, May 20). Blackberry Services Go Offline in Pakistan. Retrieved September 19, 2013, from ProPakistani: http://propakistani.pk/2010/05/20/blackberry-services-go-offline-in-pakistan/
87. Tanveer, R. (2010, June 1). Facebook access restored. Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/17751/facebook-access-restored/
88. PTI. (2010, May 27). Pakistan lifts ban on YouTube. Retrieved September 19, 2013, from Times of India: http://articles.timesofindia.indiatimes.com/2010-05-27/pakistan/28304621_1_blasphemous-caricatures-blasphemous-material-sacrilegious-content
89. Qamar Zaman, S. P. (2012, May 21). Social media censorship: 12-hour ban leaves Twitterati in a quandary. Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/381885/social-media-censorship-12-hour-ban-leaves-twitterati-in-a-quandary/
90. Siddiqui, T. (2013, September 19). Pakistan's YouTube ban, 1 year later. Retrieved September 29, 2013, from The Christian Science Monitor: http://www.csmonitor.com/World/2013/0919/Pakistan-s-YouTube-ban-1-year-later
91. Rana Tanveer, W. D. (2013, September 19). LHC refers YouTube ban case to larger bench. Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/606418/lhc-refers-youtube-ban-case-to-supreme-court/
92. PTA bans Ahmadi website. (2012, July 6). Retrieved September 19, 2013, from The Nation: http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/lahore/06-Jul-2012/pta-bans-ahmadi-website
93. Ban on Shia website: Police disperse protest rally in Karachi. (2012, July 17). Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/409505/ban-on-shia-website-police-disperse-protest-rally-in-karachi/
94. After Rehman Malik's efforts, Shia website unblocked. (2012, July 18). Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/409987/malik-orders-fia-to-investigate-banned-shia-website/
95. Walsh, D. (2011, March 29). Pakistan's secret dirty war. Retrieved September 29, 2013, from The Guardian: http://www.theguardian.com/world/2011/mar/29/balochistan-pakistans-secret-dirty-war

spreading 'misinformation'[96]. An OpenNet Initiative study in 2007 noted that, "internal security conflicts were a strong focus for filtering: all web sites tested relating to independence (for example, http://www.balochunitedfront.org/) and human rights (for example, http://balochestan.com) in the province of Balochistan were blocked."[97]

The number of blocked Baloch websites was expanded in 2009[98], and in 2010, authorities blocked The Baloch Hal, the first English language news website focused on Balochistan. By 2012, many websites, blogs and YouTube videos focused on the Balochistan conflict were blocked, although the exact number is not known due to a lack of transparency on the part of the PTA[99].

Aside from Balochistan, there has been multiple instance of content being blocked to stem information creating a perceived negative image of politicians or the military. The website of the Lal Masjid (Red Mosque) was blocked in 2007[100] – a time when the government led an operation against the mosque, resulting in at least 100 deaths[101]. A YouTube video depicting Pakistan's Naval Chief misusing his power to grab land was blocked in 2008[102]. In 2010, a block was placed on a YouTube video depicting the then President Asif Ali Zardari yelling "shut up" during a public gathering[103]. Rolling Stone Magazine's website was blocked in 2011 after a blog post discussing Pakistan's "insane military spending" was published[104]. In 2013, pop band Beygairat Brigade's song Dhinak Dhinak, which touched upon the military's powers, was blocked on Vimeo[105].

While some blocks have been temporary in nature, other have lasted years.

1.2 CRIMINALISING LEGITIMATE EXPRESSION

Pakistan is a signatory to the UN Universal Declaration of Human Rights, of which Article 19 states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[106]

Freedom of speech is also enshrined in Article 19 of the Pakistan Constitution with some restrictions imposed, "in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, or incitement to an offence."[107]

Ignoring these two standpoints on freedom of expression, the state has increasingly criminalised legitimate expression, while multiple laws that use vague, ill-defined or broad terminology exist to provide cover for such acts.

The Pakistan Telecommunications (Re-organization) Act 1996 gives the government broad regulatory powers in the name of protecting "national security", and criminalises vague offenses, such as banning the distribution of "false" or "fabricated" information, indecent materials or causing "mischief". A detailed analysis of the act by Article 19 – a London-based human rights organization – found that there are "many provisions which are incompatible with Pakistan's obligations under international law and violate citizens' rights of freedom of expression, access to information and protection of privacy." The report notes that the act has been cited as the legal basis for "numerous violations of freedom of expression, including the indiscriminate and unlawful blocking of web pages, filtering of communications systems based on keywords, the stopping of internet services using encryption and the ordering of mass surveillance of communications systems."[108] In all, the Act's vague definitions allow for the banning of pornography, blasphemy, anti-state content and a vast range of material that would impinge on fundamental rights including freedom of expression and right to information.

Section 124-A of the Pakistan Penal Code addresses sedition in broad terms, carrying a maximum sentence of life imprisonment and a fine for whoever is "found to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Federal or Provincial Government." The term "disaffection "has been explained to include "disloyalty and all feelings of enmity". As it stands, this section applies to the blocking of websites of Baloch and Sindhi Nationalists, along with other groups and individuals criticizing the govern-

96. Baloch websites banned. (2006, April 28). Retrieved September 19, 2013, from Daily Times: http://www.dailytimes.com.pk/default.asp?page=2006%5C04%5C28%5Cstory_28-4-2006_pg7_5
97. Internet Filtering in Pakistan in 2006-2007. (2007). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/studies/pakistan2007
98. Janjua, F. (2009, August 17). PTA goes ProPakistani - Starts Banning Anti-Pakistan Baloch Websites. Retrieved September 19, 2013, from ProPakistani: http://propakistani.pk/2009/08/17/pta-goes-propakistani-starts-banning-anti-pakistan-baloch-websites/
99. Waking up to the war in Balochistan. (2012, February 29). Retrieved September 19, 2013, from BBC News: http://www.bbc.co.uk/news/world-asia-17029159
100. Wasim, A. (2007, April 7). Lal Masjid's website blocked. Retrieved September 19, 2013, from Dawn: http://beta.dawn.com/news/241139/lal-masjid-s-website-blocked
101. Hasan, S. S. (2007, July 27). Profile: Islamabad's Red Mosque. Retrieved September 19, 2013, from BBC News: http://news.bbc.co.uk/2/hi/6503477.stm
102. Ahmad, S. (n.d.). Internet Censorship in Pakistan - Naval Chief misusing his powers. Retrieved September 19, 2013, from Association for Progressive Communications: http://www.apc.org/en/blog/freedom/asiapacific/internet-censorship-pakistan-naval-chief-misusing-
103. James, M. (2010, February 7). 'Shut Up'? Pakistan President's Outburst Scrubbed From 'Net. Retrieved September 19, 2013, from ABC News: http://abcnews.go.com/blogs/headlines/2010/02/shut-up-pakistan-presidents-outburst-scrubbed-from-net/
104. York, J. C. (2011, July 26). Pakistan escalates its internet censorship. Retrieved September 19, 2013, from Al Jazeera: http://www.aljazeera.com/indepth/opinion/2011/07/201172511131058991 2.html
105. Targeting the army?: Beygairat Brigade's new song partially banned in Pakistan. (2013, April 27). Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/541274/targeting-the-army-beygairat-brigades-new-song-partially-banned-in-pakistan/
106. The Universal Declaration of Human Rights. (n.d.). Retrieved September 27, 2013, from United Nations: http://www.un.org/en/documents/udhr/index.shtml#a19
107. Chapter 1 Fundamental Rights - Constitution of Pakistan. (n.d.). Retrieved September 27, 2013, from Pakistani: http://www.pakistani.org/pakistan/constitution/part2.ch1.html
108. (2012). Pakistan: Telecommunications (Re-organization) Act Legal Analysis. Article 19.

ment, calling for greater autonomy, or secession from the state. While there have not been any recorded cases of citizens being arrested on sedition grounds for online content, this section of the penal code gives the state the option to arrest those producing or disseminating content defined under the terms above.

The Anti-Terrorism Act 1997 is problematic for its lack of detailed definition of what constitutes the spread of terror or sectarian hatred, particularly in relation to the internet. The act has no mention of the internet, yet is part of the PKNIC's *(see Section 2.2.1)* policy for .PK domain registration, wherein PKNIC can reject a domain registration application for being in contravention of the Anti-Terrorism Act.

The Defamation Ordinance 2002 and Defamation Amendment Act 2004, which includes laws on slander and libel, also extend to the online space. Punishments under the laws can include a fine as well an imprisonment. While there are no known cases of online defamation, the laws lack specifics with regards to the internet.

1.3 IMPOSITION OF INTERMEDIARY LIABILITY

With 50 ISPs operating in Pakistan, greater internet penetration, and rapid expansion of locally operated sites featuring e-commerce and user generated content, the need to address imposition of intermediary liability and protection from intermediary liability is clear.

Since Pakistan has no specific laws concerning intermediary liability, the PTA has ordered ISPs to block and filter access to specific websites in the past by drawing on a cluster of existing laws that very loosely apply to the internet, or do not mention the internet at all *(See Section 1.1)*. ISPs face license suspensions for failing to carry out PTA orders.

Instances of sites being blocked or banned for hosting user content deemed 'blasphemous', 'anti-state' or 'pornographic' have become routine in the online space. Examples extend from the blanket ban on Blogger.com, to the blocking of the Baloch Hal website for hosting opinion pieces and news articles on the Balochistan crisis, to the partial block of torrent sites and most critically, the ban on Facebook and YouTube for hosting blasphemous content *(see Section 1.1)*.

The ban on Facebook was reportedly resolved through an agreement between Facebook and the government whereby the social network would block parts of Facebook for Pakistani users[109] in what may constitute state-led imposition of intermediary liability on the network. The PTA Director General (S&D), claimed in court proceedings on July 4, 2013 that Pakistan had an existing "arrangement" with Facebook, which allows them to have "undesirable" content and pages blocked as per directions from the authority. Such requests were confirmed by a Ministry of Information Technology officer[110].

The 2012 ban on YouTube has been significantly more complex. During the YouTube case in the Lahore High Court, Google submitted a written submission requesting that the government introduce intermediary liability protection for online platforms, and establish a clear notice-and-take-down-mechanism based on the Organisation for Economic Co-operation and Development guidelines[111]. Without the establishment of such protection and guidelines, Google would be unable to operate in Pakistan and offer a localized version of YouTube, which would allow for the blocking of specific videos on the government's request.

The lack of an existing policy and laws specific to intermediary liability protection for ISPs and companies operating online represents a challenge, which, unaddressed, is negatively impacting access to the internet, multiple facilities and services for users, greater technological development and importantly, fundamental rights to freedom of expression and right to information.

1.4 DISCONNECTING USERS FROM THE INTERNET

Most cases of mass disruption of internet access in the past have been related to technical faults in the undersea cables that carry a majority of Pakistan's traffic[112]. More worryingly, disconnection of users from the internet has focused on mobile phone services in connection to either blasphemy or terrorism.

In 2010, Internet services were cut off for all BlackBerry phone users in Pakistan after the PTA ordered telcos to block Facebook for hosting "Draw Prophet Muhammad Day"[113] *(See Section 1.1)*. Later in 2012, the trend of blocking mobile services en masse, and consequently cutting access to internet from mobile devices, began.

109. Ahmad, S. (2013, July 17). Facebook's secret censorship deal with the Pakistan government - an open letter. Retrieved September 21, 2013, from Bytes For All: http://content.bytesforall.pk/node/107
110. Jamal Shahid, M. A. (2013, August 16). Censoring social media: Govt caught between fans and foes. Retrieved September 21, 2013, from Dawn: http://dawn.com/news/1036144/censoring-social-media-govt-caught-between-fans-and-foes
111. Sharma, M. (2013, September 16). Pakistani Activists Smell A Mole In Government's Proposed YouTube Filtering Plan. Retrieved September 21, 2013, from Tech Crunch: http://techcrunch.com/2013/09/16/pakistani-activists-smell-a-mole-in-governments-proposed-youtube-filtering-plan/
112. Baloch, F. (2013, March 28). Underwater cable damaged: Internet speed plummets by 60% nationwide. Retrieved September 21, 2013, from The Express Tribune: http://tribune.com.pk/story/527643/underwater-cable-damaged-internet-speed-plummets-by-60-nationwide/
113. Yasir, M. (2010, May 22). Internet services suspended on Blackberry handsets: Cell phone operators incurring losses after Internet blockade. Retrieved September 22, 2013, from Daily Times: http://www.dailytimes.com.pk/default.asp?page=2010%5C05%5C22%5Cstory_22-5-2010_pg5_4

The entire province of Balochistan was cut off from mobile services on the national celebration of Pakistan Day 2012 by the PTA "in order to implement national security policy"[114]. Members of civil society including organizations such as Bytes for All *(see Section 3.1)* termed the blockade a continuation of oppression of the Baloch people and the nationalist movement[115].

> "The disconnection of mobile services is a disturbing new trend that could have far-reaching, negative implications for the future growth of the internet, as mobile phones present the greatest potential for internet access in the country

The suspension of cellular services during religious and political events has become the norm, particularly in urban centres such as Quetta and Karachi. In 2013, the interior minister Rehman Malik justified the closure of cellular services by stating that mobile phones were being used by terrorists to trigger bombs[116]. In one instance, PTCL's wireless internet services were also suspended[117]. The Sindh High Court took notice of the incidents and issued notices to the PTA and Interior Ministry. The PTA's lawyer told the courts that mobile service suspension was in "the national interest"[118].

The government has cited Article 148 of the Constitution as justification for the blocking of cellular services for hours across multiple cities, claiming credible intelligence of a terrorist threat[119]. Article 148 (3) states, "It shall be the duty of the Federation to protect every Province against external aggression and internal disturbances and to ensure that the Government of every Province is carried on in accordance with the provisions of the Constitution."

The suspension of services has also been justified under section 54(3) of the Pakistan Telecommunication (Re-organisation) Act, titled, "National Security". Its states that, "Upon proclamation of emergency by the President, the Federal Government may suspend or modify all or any order or licences made or issued under this Act or cause suspension of operation, functions or services of any licensee for such time as it may deem necessary." This section of the act provides legal cover for any decision by the government to disconnect users from telecommunication services or the internet.

The disconnection of mobile services is a disturbing new trend that could have far-reaching, negative implications for the future growth of the internet, as mobile phones present the greatest potential for internet access in the country *(see Section 1.0)*.

1.5 CYBER ATTACKS

Cyber-attacks have been a part of Pakistan's online space since over a decade, and almost entirely in connection with neighbouring India. The online cross-border 'warfare' began after New Delhi's nuclear weapons test in 1998,and has persisted due to conflict over disputed Kashmir, among other issues.

Most of the reported attacks fall under 'hacktivism' i.e. political hacking to promote an ideological viewpoint. Generally, attacks have had a limited scope and time frame, consisting mostly of website defacement, denial of service attacks and a low level of sophistication. There have been few reported cyber-attacks that caused major security threats, data theft or actual damage to data. It is unclear whether they are conducted as part of state-sanctioned/funded operations, or by independent, ideologically motivated individuals. A 2004 report by the Institute for Security Technology Studies cites "possible ties between the hacker community and Pakistani intelligence services… it is quite possible that the government of Pakistan has made only a minimal investment in its cyber warfare program."[120]

There are no laws in Pakistan specific to cyber-attacks and hacking. The highly problematic Prevention of Electronic Crimes Ordinance 2007 was implemented for a brief period, containing harsh punishments related to cyber-attacks, but the ordinance lapsed in 2009. In its absence, the FIA has been registering cases under sections 36 and 37 of the 2002 Electronic Transaction Ordinance (ETO), which deal with violation of privacy information and damage to information systems, along with section 419 (Punishment for cheating by impersonation) of the Pakistan Penal Code[121]. FIA officials have said prosecuting under the ETO causes massive delays as the case grade is low, and "people often get away with the crime"[122].

As far back as 1998, the Indian army's website on Kashmir was defaced with political slogans by supporters of Pakistan's claim to the disputed

114. Gishkori, Z. (2012, March 23). Security: Cell phone services in Balochistan suspended on Pakistan Day. Retrieved September 22, 2013, from The Express Tribune: http://tribune.com.pk/story/354095/security-cellphone-services-in-balochistan-suspended-on-pakistan-day/
115. Communication siege in Balochistan to mark Pakistan Day 2012. (2012, March 25). Retrieved September 22, 2013, from Bytes for All: http://content.bytesforall.pk/node/45
116. Eid Milad: Mobile services to be suspended in Lahore. (2013, January 24). Retrieved September 22, 2013, from The Express Tribune: http://tribune.com.pk/story/498499/eid-milad-mobile-services-to-be-suspended-in-lahore/
117. No mobile services in Karachi, Quetta till midnight. (2012, November 23). Retrieved September 21, 2013, from The Express Tribune: http://tribune.com.pk/story/470131/no-mobile-service-in-karachi-quetta-from-1pm-till-evening/
118. Mobile suspension case: SHC issues notices to PTA, interior ministry. (2012, November 22). Retrieved September 29, 2013, from The Express Tribune: http://tribune.com.pk/story/469691/mobile-suspension-case-shc-issues-notices-to-pta-interior-ministry/
119. Bikes and phones: Rehman Malik defends ban citing intelligence. (2012, November 16). Retrieved September 22, 2013, from The Express Tribune: http://tribune.com.pk/story/466731/bikes-and-phones-rehman-malik-defends-ban-citing-intelligence/
120. (2004). Cyber warfare: an analysis of the means and motivations of selected nation states. Institute for Security Technology Studies at Dartmouth College.
121. Man sent into custody for harassing girl on Facebook. (2013, September 25). Retrieved September 27, 2013, from The Express Tribune: http://tribune.com.pk/story/608681/cyber-crime-man-sent-into-custody-for-harassing-girl-on-facebook/
122. Zeeshan, O. (2011, March 24). Investigators suffering from absence of law. Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/136794/investigators-suffering-from-absence-of-law/

territory[123]. This form of 'hacktivism' or political hacking has been led by anonymous groups of allied hackers like the Pakistan Hackerz Club (PHC) which defaced hundreds of Indian sites in 2000[124] , or the Anti-India Crew and GFORCE-Pakistan. While focused on India, groups like GFORCE-Pakistan also supported other causes like the Palestinian intifada, Afghanistan and Osama Bin Laden[125]. A report by the Institute for Security Technology Studies noted that Pakistani hackers had defaced over 400 Indian websites from 1999 to 2001[126]. It also stated that, "In the case of the Bhabha Atomic Research Centre, five megabytes of possibly sensitive nuclear research or other information was reportedly downloaded."

The trend of conducting cyber-attacks across the border fluctuated over the years, with the addition of other hacker alliances including Silver Lords, World's Fantabulous Defacers and later, the Pakistan Cyber Army and PakBugs. In response, Indian hacker alliances including the Indian Snakes, Hindustan Hackers Association, Indian Hackers Club and the Indian Cyber Army formed to carry out similar attacks on Pakistani sites. The Pakistan Computer Emergency Response Team PakCERT cites over 1,600 Pakistani sites defaced from 1999 to 2008, including many government websites[127] .

In one instance in 2012, Bangladeshi hackers defaced the Punjab Assembly's website, demanding that the government take action against a Pakistani hacker who had allegedly been defacing Bangladeshi sites[128].

The FIA has been active in arresting hackers since 2006[129]. In 2010, the FIA's Cyber Crime Wing arrested a hacker on charges of hacking the personal website of the then President Asif Ali Zardari[130]. The same year, the FIA arrested five members of PakBugs, involved in defacing thousands of websites and online fraud[131]. Two teenagers linked to the Pakistan Cyber Army were also arrested for defacing the Supreme Court website[132].

Aside from the online Pak-India conflict, cyber-attacks within Pakistan are increasingly aimed at e-commerce sites and unsecure telecommunication networks[133]. Both hacktivism and attacks on online businesses pose a real threat that needs to be addressed, both legislatively and through action by the security apparatus or relevant agencies. The issue has been taken up by the Senate Committee on Defence and Defence Production, which aims to create a national policy on cyber security *(see Section 2.3.1)*.

1,600

Pakistani sites were defaced from 1999 to 2008 by internet 'hacktivists', including many government websites.

1.6 SURVEILLANCE AND LAWFUL INTERCEPT

Pakistan's surveillance of both the internet and telecom networks has expanded in a move to monitor and control all communication, regardless of fundamental freedoms defined in the Constitution. The state has tried to do this technologically as well as legislatively in recent years.

With the creation of the Pakistan Internet Exchange (PIE) in 2000, the government successfully routed a majority of Pakistan's internet traffic through a single core backbone with limited gateways, which consequently allows for relatively easy access to monitoring internet packets.

Reports indicate that PIE can store email data, and allows the monitoring of all incoming and outgoing traffic[134]. Pakistan is also reportedly a customer of US-based technology firm Narus[135], which allows for internet traffic monitoring and inspection[136]. In 2013, Canada-based Citizen Lab, based at the Munk School of Global Affairs, University of Toronto found a FinFisher Command and Control server- surveillance technology criticised internationally for undermining citizens' privacy rights - on PTCL's network. While it is not confirmed if the government is using the server for surveillance, or was aware of its presence, the existence

123. Havely, J. (2000, February 16). When states go to cyber-war. Retrieved September 20, 2013, from BBC News: http://news.bbc.co.uk/2/hi/science/nature/642867.stm
124. Israel lobby group hacked. (2000, November 3). Retrieved September 20, 2013, from BBC News: http://news.bbc.co.uk/2/hi/middle_east/1005850.stm
125. Anderson, K. (2001, October 23). Hacktivists take sides in war. Retrieved September 20, 2013, from BBC News: http://news.bbc.co.uk/2/hi/americas/1614927.stm
126. (2001). Cyber attacks during the War on Terrorism: A predictive analysis. Hanover: Institute for Security Technology Studies at Dartmouth College.
127. Pakistan Computer Emergency Response Team. (2008). Retrieved September 20, 2013, from PakCERT: http://www.pakcert.org/defaced/stats.html
128. Online. (2012, December 10). Bangladeshi hackers hack PA website, Pakistani hackers hit back. Retrieved September 20, 2013, from Pakistan Today: http://www.pakistantoday.com.pk/2012/12/10/city/lahore/bangladeshi-hackers-hack-pa-website-pakistani-hackers-hit-back/
129. Chickowski, E. (2006, December 11). Pakistanis make arrest in ransom-hacking case. Retrieved September 20, 2013, from SC Magazine UK: http://www.scmagazineuk.com/pakistanis-make-arrest-in-ransom-hacking-case/article/106765/
130. 'Penetrator' arrested on charges of hacking Zardari's website. (2010, December 6). Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/86576/penetrator-arrested-on-charges-of-hacking-zardaris-website/
131. AFP. (2010, July 8). Gang of website hackers busted. Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/26477/gang-of-website-hackers-busted/
132. Khan, I. A. (2010, October 27). Two boys arrested for hacking SC website. Retrieved September 20, 2013, from Dawn: http://archives.dawn.com/archives/75158
133. Ashraf, G. (2011, April 3). Cyber wars. Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/140431/cyber-wars/
134. Pakistan. (2012, August 6). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan
135. Freedom on the Net 2012: Pakistan. (2012). Retrieved September 15, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/2012/pakistan
136. Freedom on the Net 2012: Pakistan. (2012). Retrieved September 15, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/2012/pakistan

of the server has caused rights groups to demand an investigation into whether citizens are being spied upon [137].

In the existing legal frame work, online surveillance and lawful intercept is carried out by the PTA and multiple security agencies, which follow guidelines set out by the government, courts and Ministry of Information Technology (MoIT). Law enforcement and intelligence agencies can conduct surveillance and monitor content either independently, or turn to the FIA and PTA for assistance. Under the lapsed PECO, ISPs were required to retain traffic data for a minimum of 90 days and could be required to monitor and collect real-time data and provide information to the government confidentially[138]. There was no specification for what actions would constitute grounds for monitoring and data collection. Despite the ordinance lapsing, the practice was still active as of mid-2012[139].
A number of existing laws allow for monitoring and surveillance of the internet.

> "In giving security agencies wide-ranging technological means and legislative cover to access citizens' private data, the likelihood of misuse is high. While there is a need for laws governing internet surveillance, the current ad-hoc system gives the state powers that could be used for harassment and intimidation.

The Investigation for Fair Trial Act 2013 gives Pakistan's security agencies the authority to collect evidence "by means of modern techniques and devices" that will be accepted in a court in cases registered under five security-related laws. Surveillance can include, "data, information or material in any documented form, whether written, through audio visual device, CCTV, still photography, observation, or any other mode of modern devices or techniques obtained under this Act." Along with surveillance, agencies can be authorized to intercept, "e-mails, SMS, IPDR (Internet Protocol Detail Record) or CDR (Call Detail Record) and any form of computer based or cell phone based communication and voice analysis. It also includes any means of communication using wired or wireless or IP (internet protocol) based media or gadgetry."[140] The law applies to Pakistanis in the country and abroad.

The Fair Trial Act allows agencies to collect data from 'service providers' including telecom operators and ISPs, with failure to comply in such demands resulting in fines of up to Rs10 million and imprisonment for two years. The Act also gives service providers legal indemnity from involvement in collecting and handing over customers' private data. The actual process of obtaining a warrant is outlined: officials must submit a report to the agency's department head or a BPS-20 officer, and the approved report is then submitted to a judge. The report is then reviewed, and a warrant is issued by the judge in their chamber – a process which will not be a public record.

The Fair Trial act has been criticized by legal experts for its lack of depth, lack of clear definitions, a flawed process for obtaining warrants and an imbalance against both security agencies and citizens due to a lack of safeguards[141]. The act uses vague, ambiguous terms to describe the proof a security agency would need to obtain a warrant. The legal experts also expressed fear that the bill could be misused by security and intelligence agencies for political purposes, while it could also affect the fundamental rights of citizens.
In addition to the Fair Trial Act, the Pakistan Telecommunications (Re-organization) Act 1996 gives the government broad surveillance powers under vague, undefined terminology. Section 54 of the Act allows the government to authorise any person or persons to intercept calls and messages, or to trace calls through any telecommunication system in "the interest of national security or in the apprehension of any offence."

In 2011, the PTA ordered all ISPs and mobile phone companies to ban encryption and virtual private networks (VPNs) in Pakistan as an anti-terrorism measure, based on the Monitoring & Reconciliation of International Telephone Traffic Regulations 2010[142]. In theory, the law would allow easier surveillance of unencrypted data for the government in what is tantamount to a breach of privacy. It is unclear as to what extent this ban has been implemented, as encryption is used regularly to provide secure banking and e-commerce, as well as to bypass the blockage of websites.

In October 2013, the provincial government of Khyber-Pukhtunkhwa ordered the collection of data from internet cafes in the province, ordering the police to keep records of internet cafe users and recommended

137. FAQ: What is FinFisher, What is it doing in Pakistan? (2013, May 18). Retrieved September 26, 2013, from Digital Rights Foundation: http://digitalrightsfoundation.pk/faq-what-is-finfisher-what-is-it-doing-in-pakistan/
138. Prevention Electronic Crimes Ordinance. (2007, December 31). Gazette of Pakistan. Islamabad, Pakistan.
139. Freedom on the Net 2012: Pakistan. (2012). Retrieved September 15, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/2012/pakistan
140. Investigation for Fair Trail Act. (2013, February 22). Gazette of Pakistan. Islamabad, Pakistan.
141. Imtiaz, S. (2012, October 22). Pakistan's 'patriot act'?: How fair is the new trial bill? Retrieved September 20, 2013, from The Express Tribune: http://tribune.com.pk/story/454973/pakistans-patriot-act-how-fair-is-the-new-trial-bill/
142. Asia Pacific: Free expression and law in 2011. (2012, April 5). Retrieved September 20, 2013, from Article 19: http://www.article19.org/resources.php/resource/3026/en/asia-pacific:-free-expression-and-law-in-2011

installation of hidden cameras. The government opted for this extreme measure citing reports of a rise in threatening emails in the province[143].

In giving security agencies such wide-ranging technological means and legislative cover to access citizens' private lives and conversations, the likelihood of misuse and abuse is high. While there is a need for laws governing internet surveillance, the current ad-hoc system lacks clear definitions, transparency, accountability and oversight mechanisms, giving the state powers that could be used for harassment and intimidation.

1.7 DATA PROTECTION

There are no laws in Pakistan that specifically deal with data protection on the internet. Article 14(1) of the Pakistan Constitution ensures the right to privacy, stating that "the dignity of man and, subject to law, the privacy of home, shall be inviolable." The Constitution also states in Article 8 that laws are void that are inconsistent or in derogation of fundamental rights.

The 2002 Electronic Transaction Ordinance (ETO) contains sections dealing with violation of privacy and damage to information systems that may apply to online data protection. According to section 36 of the ordinance, "Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both."[144]

1.8 NET NEUTRALITY

There is no existing legislation or regulatory framework that specifically addresses net neutrality in Pakistan. While the issue of non-discrimination in the handling of internet data would fall under the PTA, which regulates both the telecom industry and internet, there has been little to no debate on the matter.

ISPs such as PTCL have, in the past, arbitrarily opted to slow down access to torrents or blocked Skype, reportedly because such services could be impacting their revenues[145]. The PTA strictly regulates Voice over IP (VoIP) and every ISP has to sign an Electronic Information Services (EIS) or Non Voice Communication Network Services (NVCNS) license that states, "The licensee shall be responsible to make sure that no transmission of voice takes place on the data network through his licensed Electronic Information Services." The PTA claims the "legality of VoIP comes into question only when someone exploits its benefits for illegal commercial purposes". The PTA orders regarding VOIP were criticized by members of the IT industry including ISPAK[146] .

1.9 GOVERNMENT ENGAGEMENT AT THE INTERNATIONAL LEVEL

Pakistan has been participating in the global discussion around the Internet, information society and other related issues, although implementation of global standards and practices has been limited to non-existent. The United Nations – International Telecommunication Union (ITU) initiated the World Summit on Information Society (WSIS) in 2001, aiming to bridge the digital divide and strengthen Information Society at a global level[147]. The first Geneva phase of the WSIS was attended by a contingent from Pakistan headed by the then Prime Minister Zafarullah Khan Jamali. Ambassador Masood Khan led the Pakistan delegation from the Pakistan Mission in Geneva for the second phase of WSIS held in Tunis in 2005. Ambassador Masood Khan was also part of the Working Group on Internet Governance (WGIG)[148] and instrumental in developing the idea of a multi-stakeholder annual Internet Governance Forum. The PTA was also part of preparatory meetings for the World Summit on Information Society. Pakistan is active at the ITU and regularly participates in all its meetings and summits.

Pakistan adopted the WSIS Geneva Declaration, WSIS Plan of Action[149] 2003 and Tunis Agenda 2005[150]. However, none of the commitments could be translated in the policy-making processes in the country. Pakistan also regularly attends the Governmental Advisory Committee (GAC) meetings at ICANNS but the multi-stakeholder governance model is non-existent in the country.

Recently, the UN Human Rights Council has taken up a number of Internet related issues through discussions facilitated via reports by the UN Special Rapporteur on Freedom of Expression, Opinion & Speech. Pakistan's

143. (K-P govt asks IGP to keep check on internet cafes, 2013)
144. Electronic Transactions Ordinance, 2002. (2002). Gazette of Pakistan. Islamabad, Pakistan.
145. Attaa, A. (2013, March 13). PTCL Starts Blocking the Torrents. Retrieved September 22, 2013, from ProPakistani: http://propakistani.pk/2013/03/13/ptcl-blocking-torrents/
146. Ghafoor, K. (2005, November 15). VoIP Regulation in Pakistan: A General Perspective. Retrieved September 22, 2013, from Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?option=com_content&view=article&id=668:voip
147. About WSIS. (n.d.). Retrieved October 1, 2013, from World Summit on the Information Society: http://www.itu.int/wsis/basic/about.html
148. About WGIG. (n.d.). Retrieved October 1, 2013, from Working Group on Internet Governance: http://www.wgig.org/About.html
149. Plan of Action. (2003, December 12). Retrieved October 1, 2013, from WSIS: http://www.itu.int/wsis/docs/geneva/official/poa.html
150. Tunis Agenda for the Information Society. (2005, November 18). Retrieved October 1, 2013, from WSIS: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

role at this global forum has been particularly predatory and anti-human rights[151]. Pakistan has also been part of the first and second cycle of the United Nations Universal Periodic review of human rights. Bytes For All Pakistan was actively involved in this engagement[152], and the organization has played a major role in global and local advocacy as a regional network since 1999. Bytes For All Pakistan also engaged globally by calling for an end to the blocking of websites by the government through an Allegation Letter to UN Special Rapporteur on Freedom of Expression Frank La Rue in 2013[153].

2.0 SUMMARY OF MAIN FINDINGS

Pakistan is currently facing multiple challenges related to the internet in terms of further growth and proper governance in line with international laws and the country's own Constitution.

> "Large swathes of the online space have been blocked on subjective grounds ranging from 'national security' to 'obscenity', 'anti-state' and 'blasphemy'. The wide-ranging blocks have forced citizens to turn to proxy servers, VPNs and other online tools to get around state censorship.

The switch-over to high speed internet has not occurred as the government had envisioned, and while the number of broadband users does continue to grow, they are almost entirely located in urban centres, catering to a minority of internet users. Until the government and ISPs can strategize and act to spread the internet to rural areas, Pakistan will see slow growth in terms of internet penetration. One vital part of this strategy could be a switch from the slow EDGE to 3G or 4G cellular networks, but this process has already been delayed over two years due to government infighting and irregularities in the tendering practice. Additionally, the government has recently taken to implementing region-wide blocks of mobile services, and consequently internet access as an anti-terrorism measure; a dangerous, stepping stone to greater control over all communication in the country.

The state's growing need to police cyberspace has led to numerous violations of fundamental rights, including freedom of speech, access to information and right to privacy. The process of arbitrary blocking and filtering has increased over the last decade, and has been justified by referencing a wide set of existing laws, many of which make no direct reference to the internet, or contain vague, ambiguous definitions. As a result, large swathes of the online space have been blocked on subjective grounds ranging from 'national security' to 'obscenity', 'anti-state' and 'blasphemy'. The wide-ranging blocks have forced citizens to turn to proxy servers, VPNs and other online tools to get around state censorship.

The state has also systematically worked to legitimize the invasion of citizens' online privacy. This has been done through government orders like the banning of encryption and VPNs in Pakistan, or by means of legislation like the Fair Trial Act, which allows security agencies to closely monitor and spy on internet users, along with accessing their private data – all in the name of countering terrorism. While there is a great need for laws that deal with use of the internet in connection to illegal activities, the existing legislation and practices are flawed and open to misuse and human rights violations.

Both online surveillance and blocking and filtering have been assisted technologically by US and Canadian companies. The government is reportedly a customer of US-based technology firm Narus[154] for online surveillance, uses Canada-based Netsweeper's filtering software to block access to sites and in one troubling instance, a FinFisher Command and Control server that could be used for surveillance was found on a local ISP's network.

Cyber-attacks are a frequent feature of Pakistan's online space. They have largely focused on ideological, politically motivated hacking, or 'hacktivism', but attacks are slowly shifting towards targeting ecommerce and online business, which presents a new threat to an industry which is still in its infancy. The bigger threat to state security also cannot be ruled out, but so far, Pakistan has done little to address the issue or develop a plan of action beyond relying on its existing security apparatus to counter such threats.

In the existing landscape, there is little room, though increasing need, for debate or legislation on more complex issues such as intermediary liability protection, data protection and net neutrality.

151. Online surveillance becomes a priority for the Human Rights Council, as Pakistan joins the wrong side of the debate. (2013, September 25). Retrieved October 1, 2013, from Privacy International: https://www.privacyinternational.org/press-releases/online-surveillance-becomes-a-priority-for-the-human-rights-council-as-pakistan-joins
152. Bytes for All, P. a. (2012). Universal Periodic Review 14th Session – Pakistan Stakeholder Report.
153. Bytes for All, P. M. (2013, March 13). Letter of Allegation regarding the blocking of websites by the Government of Pakistan. Retrieved November 11, 2013, from Bytes For All Pakistan: http://content.bytesforall.pk/sites/default/files/Bytes%20for%20All%20and%20MLDI%20Letter%20of%20Allegation%20website%20blocking%20Pakistan.pdf
154. Freedom on the Net 2012: Pakistan. (2012). Retrieved September 15, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/2012/pakistan

2. INTERNET GOVERNANCE PROCESSES AND POWER PLAYERS

2.1 RELEVANT MINISTRIES

2.1.1. Pakistan Telecommunication Authority

Established in January 1997 under the Telecom Reorganization Act 1996, the PTA is the main regulatory and license issuing body overseeing the internet and telecom industry in Pakistan. It also functions to promote the spread of internet and telecommunication services, and make recommendations on matters of policy. The PTA is at its core, a government entity, as its chairman and members are appointed by the federal government, while the body reports to the Ministry of Information Technology and Telecommunication (MoIT)[155] . Working in close coordination with PTCL and the FIA, the authority regulates online activities under the direction of the government, the Supreme Court, and the MoIT.

Given the PTA's direct link to the government, international human rights organizations, free expression groups, and experts have expressed reservations about the PTA's governance structure, openness, and independence as a regulatory body[156] . In recent years, the PTA has seen a churn of appointments and resignations, forcing the Supreme Court to order the government to resolve the issue in 2013. Officials expressed reservations over the transparency of the appointment process[157].

In terms of blocking and filtering content, the authority relies primarily on maintaining a blacklist of URLs that are blocked at both the internet exchange point (IXP) through PIE and by the ISPs. A 2013 report by Citizen Lab revealed that PTA has been using Canada-based Netsweeper technology for blocking and filtering online content[158]. Netsweeper has categorized over five billion URLs in total, adding approximately 10 million new URLs every day, giving the PTA potentially sweeping censorship powers.

2.1.2. Ministry of Information Technology

The federal MoITis charged with initiating and launching IT and Telecommunications programs across Pakistan, along with establishing policies and legal framework and infrastructure for ICTs. The Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW) was created within the MoIT in 2006 to evaluate online content and requests for blocking websites, and to give recommendations to the ministry for issuance of filtering and blocking orders. The committee is administered by the secretary of the MoIT and comprises of representatives of ministries of interior, cabinet, information and broadcasting and security agencies[159]. Information regarding the names of past and existing members of the IMCEW is not publicly available.

Directives to block content are typically issued from the government or the Supreme Court through the IMCEW to the MoIT and the PTA, who then pass the orders to individual ISPs. However, because there is no specific legal framework, directives can be given directly to the PTA and ISPs to block material without going through the IMCEW. A Deregulation Facilitation Unit is responsible for addressing the grievances that Internet users may have with this censorship body.

In February 2012 the research arm of the MoIT, the National Information & Communication Technology Research and Development Fund made a public bid for a system that could block and filter up to 50 million websites. The bid was dropped later that year after a public outcry and pushback from civil society organizations[160].

2.1.3 Federal Investigation Agency

Established in 1974, the FIA is an autonomous federal institution that investigates and undertakes operations against terrorism, federal crimes, fascism, smuggling as well as copyright infringement and other specific crimes. The Director General of the agency is appointed by the Ministry of Interior. The government turns to agencies like the FIA to conduct surveillance and monitor content online.

The FIA had established the National Response Centre

155. Pakistan Telecommunication (Re-organization) Act. (1996, October 17). The Gazette of Pakistan. Islamabad, Pakistan.
156. Freedom on the Net 2012: Pakistan. (2012). Retrieved September 15, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-net/2012/pakistan
157. Baloch, F. (2013, September 24). Telecom authority: In tune with SC orders, members may be appointed this week. Retrieved September 24, 2013, from The Express Tribune: http://tribune.com.pk/story/608305/telecom-authority-in-tune-with-sc-orders-members-may-be-appointed-this-week/
158. O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime. (2013, June 20). Retrieved September 20, 2013, from Citizen Lab: https://citizenlab.org/2013/06/o-pakistan/
159. Iqbal, N. (2006, September 3). Body set up to block websites. Retrieved September 24, 2013, from Dawn: http://dawn.com/news/208722/body-set-up-to-block-websites
160. Rana, S. (2012, March 19). IT ministry shelves plan to install massive URL blocking system. Retrieved September 24, 2013, from The Express Tribune: http://tribune.com.pk/story/352172/it-ministry-shelves-plan-to-install-massive-url-blocking-system/

for Cyber Crimes (NR3C) which was active since 2002 in Pakistan, but it was not until the promulgation of the Prevention of Electronic Crimes Ordinance (PECO), that the agency gained greater legislative powers to investigate, prosecute and control electronic crime. The main objective of NR3C was to enforce cyber laws and deal with Internet fraud, email threats, plastic money fraud and other financial crimes[161].

While NR3C has managed to provide a single point of contact for cyber-crimes and increase awareness on the issue, it has had limited success in terms of prosecuting criminals following the lapse of PECO. National Response Centre officials have argued that in the absence of legislation, cases that are reported to the NR3C no longer fall under their jurisdiction[162]. In 2010 the Supreme Court ordered that the agency could no longer even investigate most cases. Despite these orders the NR3C has been functioning by patching together certain laws to form a type of 'selective legislation' which is used to protect powerful stakeholders *(See Section 1.1.3)*. When the victim of cybercrime is an influential person, the NR3C can and will interpret laws in such a way that his or her complaint can be investigated[163]. It is activities like this that has resulted in the FIA being called disreputable by Pakistan Muslim League-Nawaz (PML-N) and omitted from the list of agencies that could seek surveillance warrants under the Fair Trial Act[164].

2.2 OTHER RELEVANT PROCESSES AND SPACES

2.2.1 PKNIC

Established in 1992, PKNIC operates and administers the "Shared Registry System" for .pk domains[165]. It also operates and maintains the root servers for .pk domain DNS, manages the registration of .pk domains and manages, archives and disseminates public records on internet domain addresses. The company is operated as a self-supporting organization. In 2009, the transition of county code Top Level Domain (ccTLD) .pk to Pakistan was successfully completed by PKNIC in Lahore[166].

2.2.2 Pakistan Software Houses Association

The Pakistan Software Houses Association (P@SHA) is a platform representing the software industry of Pakistan. It has been actively involved in the growth of ICTs in the country, keeping track of the IT industry, and communicating with the government with regards to policy making in this area[167]. Being a key stakeholder, P@SHA's role is both of pressure group and advisor in dealing with the state. P@SHA and ISPAK *(see Section 2.3.2)* prepared a draft of the Prevention of Electronic Crimes Act 2013 in consultation with the NR3C, FIA, PTA, Telecom Operators and MoIT[168]. The draft could eventually come to fill the legislative gap left after the lapsing of the problematic Prevention of Electronic Crimes Ordinance 2007.

2.3 POWERFUL PLAYERS

2.3.1 Politicians

Politicians are key players in relation to many aspects of the existing internet landscape. The upper and lower houses of Parliament are responsible for creating and passing legislation related to the internet, which in large part determines the future of Pakistan's cyberspace. One prominent recent example is the ongoing work of the Senate Committee on Defence and Defence Production, headed by Senator Mushahid Hussain, which aims to create a national policy on cyber security. The action plan includes multiple points including the formation of a Joint Task Force for Cyber Security, new legislation, the establishment of a National Computer Emergency Response Team (PKCERT), formation of an Inter-Services Cyber Command and initiating talks among the 8-member states of SAARC particularly India to establish acceptable norms of behavior in connection to cyber security[169] .

Politicians also appoint people to head key ministries and bodies that deal with internet growth and governance such as the MoIT, PTA and FIA. They also form part of the Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW) which directly determines what online content should be blocked and filtered. As noted in section 1.1.3 and 2.1.3, most cases of successful cybercrime investigation and arrests, as well as many instances of blocking and filtering of content has been politically motivated.

Politicians and political parties also form the most vulnerable group online, because on the one hand, an open online space has chipped away and challenged their authority in recent years; while on the other hand, they face the prospect of genuine political victimization through the circulation of libelous content, hacking and resultant breaches of privacy, and increased online sur-

161. National Response Centre for Cyber Crimes(NR3C). (n.d.). Retrieved September 24, 2013, from Federal Investigation Agency: http://www.fia.gov.pk/prj_nr3c.htm
162. Javaid, M. (2012, January 17). A world without law. Retrieved September 24, 2013, from Herald: http://herald.dawn.com/2012/01/17/a-world-without-law.html
163. Javaid, M. (2012, January 17). A world without law. Retrieved September 24, 2013, from Herald: http://herald.dawn.com/2012/01/17/a-world-without-law.html
164. Asghar, R. (2012, December 20). 'Fair trial bill' passed in big compromise. Retrieved September 24, 2013, from Dawn: http://dawn.com/news/772798/fair-trial-bill-passed-in-big-compromise
165. About PKNIC. (n.d.). Retrieved September 24, 2013, from PKNIC: http://pk6.pknic.net.pk/pk5/pgAbout.PK
166. Transition of '.pk' domain completed. (2009, July 18). Retrieved September 24, 2013, from Daily Times: http://www.dailytimes.com.pk/default.asp?page=2009%5C07%5C18%5Cstory_18-7-2009_pg5_7
167. About P@SHA. (2013). Retrieved September 30, 2013, from P@SHA: http://pasha.org.pk/about/
168. Draft Policies. (n.d.). Retrieved September 30, 2013, from Ministry of Information Technology: http://202.83.164.29/moit/frmDetails.aspx?opt=misclinks&id=52
169. APP. (2013, July 12). Senate committee proposes 7-point Action Plan for Cyber Secure Pakistan. Retrieved September 28, 2013, from Dawn: http://dawn.com/news/1023706/senate-committee-proposes-7-point-action-plan-for-cyber-secure-pakistan

veillance that could result in both harassment and intimidation.

The positions of interior minister – currently the PML-N's Chaudhry Nisar Ali Khan – and that of minister of IT – currently the PML-N's Anusha Rehman – are important as the former is involved in security of the state which extends to the internet, while the latter is involved in internet growth and regulation. Lastly, politicians that head right-wing conservative religio-political parties like the Jamaat-e-Ulema Islam Fazl (JUI-F) and the Jamaat-e-Islami (JI) present a challenge to the development of a free, open internet, as they not only lobby against legislation connected to religion and specifically the blasphemy laws, but also command party workers that take out street protests in favor of internet bans.

2.3.2 Businesses

The primary business that is a major stakeholder in Pakistan's cyberspace is the ISPs. There are at least 50 operational ISPs providing internet services, of which 10 provide high-speed services[170]. The ISPs and PTCL in particular drive investment and overall growth of the internet.

The overall bandwidth in Pakistan ranges around 130,000 Mbits through four undersea cables – three controlled by Pakistan Telecommunication Company Ltd (PTCL) and one by Transworld Associates (TWA). PTCL, an ISP which is partly owned by the government, also operates the Pakistan Internet Exchange (PIE) which facilitates most of the internet traffic exchange between ISPs inside and outside the country. PIE was created in 2000 to provide a single backbone for Pakistan by providing peering points for ISPs[171] . It has three main nodes in Karachi, Lahore and Islamabad as well as over 40 smaller nodes. PTCL was the sole provider of bandwidth to the country until 2009, when the company announced that ISPs were free to buy bandwidth from third-party providers[172]. Aside from TWA, the company still controls most of the bandwidth in Pakistan.

PTCL still maintains a position of power in the market due to its partial government ownership and close coordination with the state, and due to its control over PIE and the majority of bandwidth in the country. Other big players include Wateen, Qubee, Comsats, LINKdotNET, World Call and WiTribe. ISPs also engage in regulation and monitoring of the internet on government orders *(see Sections 1.1 and 1.6)* often directly violating their customers' fundamental rights. In such a market, the ISPs were compelled to form the Internet Service Providers Association of Pakistan (ISPAK) in 1997 to provide a single platform to work on professional, infrastructural and regulatory issues as well as deal with PTA, PTCL and other ministries and organizations. ISPAK continues to work on internet-related issues today.

Pakistan is experiencing a surge in businesses that are tied to or depend on the internet for their economic activities, including some that are solely based online. The IT sector – now a $2 billion industry – is one of the major stakeholders, and parts of the industry are involved in internet policy making *(see Section 2.2.2)*. Cellular service providers operating in Pakistan – Mobilink, Telenor, Warid, Ufone and Zong – are also tied to the internet through the EDGE network that provides their customers internet connectivity, aside from various other offerings in the market. The top 100 visited sites in Pakistan include OLX Pakistan – a popular consumer to consumer marketplace –and Pakwheels – an online portal to buy and sell cars, among other online business sites[173]. These businesses can be engaged on cyber security, data privacy, arbitrary blocking and filtering, cellular service blocking and the need for protection from intermediary liability among other key issues. In particular, these businesses along with the banking sector carry out secure transactions and daily operations using encryption and virtual private networks – both of which are technically banned in Pakistan, allegedly to prevent terrorism *(see Section 1.6)*. This issue would be of paramount importance for stakeholders to resolve for the growth of online business.

Lastly, private media groups are a powerful stakeholder in the online space. Since the electronic media boom of the Musharraf era, 20 privately owned broadcasters with 89 domestic and 26 foreign channels have revolutionized the media industry, holding roughly half the national viewing audience over state-owned TV channels[174]. Cross-media ownership has led to a concentration of power among a few media groups including the Jang Group, the Dawn Media Group and the Express Media Group all of whom run sites in the top 100 visited in Pakistan[175], along with operating large social media networks. Given the lack of research and public records, private media serve as the public record of internet developments, and play an important role in

170. ISPAK. (2012, April 26). Retrieved September 15, 2013, from Internet Service Providers Association of Pakistan: http://www.ispak.pk/
171. Pakistan. (2012, August 6). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan
172. Pakistan. (2012, August 6). Retrieved September 15, 2013, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan
173. Top sites in Pakistan. (2013). Retrieved September 20, 2013, from Alexa: http://www.alexa.com/topsites/countries/PK
174. Yusuf, H. (2013). Mapping Digital Media: Pakistan. Open Society Foundations.
175. Top sites in Pakistan. (2013). Retrieved September 20, 2013, from Alexa: http://www.alexa.com/topsites/countries/PK

shaping public opinion on internet issues. They are also vulnerable to censorship by the state, and therefore vital to the debate. Given that many media groups are also publishing and airing user-generated content, the question of how intermediary liability is imposed is also one that directly impacts their business.

2.3.3 Military

Given that Pakistan has spent decades under military rule, the armed forces are major players when it comes to the internet in Pakistan. As outlined in Section 1.1.3, the blocking and filtering of content deemed anti-state, and in particular, anti-military has been witnessed many times over the last decade. An OpenNet Initiative study highlighted that the most 'substantial filtering' of content was related to conflict and security, with information on the Balochistan conflict being the primary target for blocks. The Inter-Ministerial Committee for the Evaluation of Web sites *(see Section 2.1.2)* which determines what online content is to be blocked has representatives of security agencies among its members. With such direct involvement, aany debate, action or legislation concerning the issue of internet blocks and filters would inevitably require engaging the military.

Additionally, the military and its security/intelligence agencies are directly involved in online surveillance, cybercrime and 'cyber terrorism' with broad powers under a set of existing legislation *(see Section 1.6)*.

2.3.4 Radical religious groups

Religious leaders expressing a radical or extremist viewpoint and many banned, sectarian or militant organizations are now a regular feature of Pakistan's online space. Banned groups such as Tehreek-e-Taliban Pakistan[176], Sipah-e-Sahabah, Lashkar-e-Jhangvi, Lashkar-e-Taiba and Hizbut Tahrir to name a few, use social networks, SMS and video-sharing sites to spread hate and recruit like-minded members[177]. Thousands of right-wing, extremist or even militant-run Facebook groups and pages[178], Twitter accounts, YouTube channels and websites are active and working online, and some have played a major role in creating an environment where internet filtering related to content deemed 'blasphemous' or 'obscene' cannot be questioned without the threat of street protests, harassment, imprisonment or violence.

This poses a major challenge, as such radicalized groups and their support networks cannot be engaged at any level, while their messages are counterproductive to creating a free, open and safe cyberspace.

In 2012, the Tehreek-e-Taliban shot 15-year-old BBC blogger and rights activist Malala Yousufzai in the skull in Swat valley. Malala survived the assassination attempt, and the shooting received worldwide attention. The Taliban justified the shooting by claiming Malala was spreading "negative propaganda" against Muslims[179]. Immediately after the attack, a large-scale online and SMS campaign was launched in Pakistan against Malala by extremist elements[180]. The Taliban have also threatened to bomb mobile phone shops for spreading obscenity[181], and have cracked down on CD/video stores and internet cafes with threats of violence[182].

> "Most extremist, militant online groups operate with relative impunity, facing no blocks or bans on their sites, blogs or social media accounts despite much of their content falling under hate-speech, libel, spreading sectarian hatred and calls to violence or overthrow of the government

In 2013, a university lecturer was arrested after extremist outfits alleged he shared blasphemous content on Facebook[183] while a Christian youth was forced to flee Karachi to avoid arrest for allegedly sending blasphemous text messages[184] underscoring the very real threat such groups pose, and the resultant self-censorship Pakistanis impose on themselves online.

Most of these online groups operate with relative impunity, facing no blocks or bans on their sites, blogs or social media accounts despite much of their content falling under hate-speech, libel, spreading sectarian hatred and calls to violence or overthrow of the government[185]. It is a matter of grave concern that internet regulation has not focused on local extremists, banned organizations and militants. These groups and their ideologically driven leaders are part of the challenge that needs to be addressed as increased internet penetration leads to a more diverse online Pakistani audience. The fact that these groups remain operative on-

176. AFP. (2012, December 7). Pakistani Taliban recruits via Facebook. Retrieved October 3, 2013, from The Express Tribune: http://tribune.com.pk/story/476533/pakistani-taliban-recruits-via-facebook/
177. Yusuf, H. (2013). Mapping Digital Media: Pakistan. Open Society Foundations.
178. Ahmed, I. (2010, July 8). Newest friends on Facebook? Pakistan militants. Retrieved September 26, 2013, from Christian Science Monitor: http://www.csmonitor.com/World/Asia-South-Central/2010/0708/Newest-friends-on-Facebook-Pakistan-militants.
179. Richard Leiby, M. L. (2012, October 9). Taliban says it shot Pakistani teen for advocating girls' rights. Retrieved October 3, 2013, from The Washington Post: http://www.washingtonpost.com/world/asia_pacific/taliban-says-it-shot-infidel-pakistani-teen-for-advocating-girls-rights/2012/10/09/29715632-1214-11e2-9a39-1f5a7f6fe945_story_1.html
180. Haque, J. (2012, October 15). We are not Malala, we may be the Taliban. Retrieved October 3, 2013, from The Express Tribune: http://blogs.tribune.com.pk/story/14351/we-are-not-malala-we-may-be-the-taliban/
181. AFP. (2013, March 3). Taliban threaten to bomb mobile phone shops. Retrieved October 3, 2013, from The Nation: http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/national/03-Mar-2013/taliban-threaten-to-bomb-mobile-phone-shops?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+pakistan-news-newspaper-daily-english-online%2FPolitics+(The+
182. Sherazi, Z. S. (2013). CD shops, net cafes face Taliban threat in Nowshera. Retrieved October 3, 2013, from Dawn: http://x.dawn.com/2013/02/19/cd-shops-net-cafes-face-taliban-threat-in-nowshera/
183. TTNR for sacking of BZU VC. (2013, June 22). Retrieved September 26, 2013, from The Nation: http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/national/22-Jun-2013/ttnr-for-sacking-of-bzu-vc
184. Christian boy accused of sending blasphemous texts still in hiding. (2012, November 16). Retrieved September 26, 2013, from The Express Tribune: http://tribune.com.pk/story/466395/christian-boy-accused-of-sending-blasphemous-texts-still-in-hiding/
185. Haque, J. (2013). Hate-Speech and Social Media in Pakistan. Retrieved September 26, 2013, from Jinnah Institute: http://www.jinnah-institute.org/open-democracy-initiative/699-hate-speech-and-social-media-in-pakistan-

line while large-scale blocks and bans continue suggests either a lack of political will to tackle the extremist elements, or more worryingly, political agreement and support – from both the government and citizens – for the narrative they spread.

A 2012 NOREF – Norwegian Peace Building Resource Centre – report noted that, "The risks posed by social media in Pakistan include their succumbing to the same ideological divisions that afflict Pakistani society and even becoming a haven for extremist online communication." The same report argued that social media in Pakistan is a platform for communication, but not a catalyst for change – partly due to a strong, largely independent traditional media presence, partly due to a low penetration rate and, "an increasingly conservative Pakistani society that frowns on public expressions of support for minorities and other pluralistic causes."[186]

2.3.5 Judiciary

The role of the judiciary in Pakistan has evolved since the Lawyer's Movement in 2007 led to the eventual ousting of the then President, General Musharraf. Experts[187] and critics[188] have referred to the post-2007 judiciary as one driven by 'judicial activism'. In the case of the internet, the judiciary is key, as it is a part of both online blocking and filtering and surveillance.

In multiple instances, the judiciary has ordered the government to block and filter content in connection to both pornography and blasphemy *(see Section 1.1.2)*, with perhaps the most prominent case being the ban on Facebook in 2010, where the Islamic Lawyers Association requesting a court injunction to ban the site for hosting blasphemous content. The social network was blocked for nearly two weeks by the Lahore High Court as a result[189]. Through the Fair Trial Act the judiciary is also a part of the surveillance process, as a judge is required to review and issue warrants– that are not public record – for security agencies to engage in online surveillance *(see Section 1.6)*.

The judges' ability to interpret law and maintain checks and balances on other pillars of the state could help in improving internet governance, although this potential is yet to be fulfilled.

2.4 MULTI-STAKEHOLDER GOVERNANCE

Growing internet penetration has convinced the government that online governance is an important issue, but the state lacks coherent strategies at both the local and international level. Pakistan has made little effort to make internet governance multilateral, transparent and democratic.

While Pakistani representatives participated in WGIG and WSIS *(see Section 1.9)* 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[190], 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.

Actual efforts to take on board multiple stakeholders in the governance process are far and few. P@SHA *(see Section 2.2.2)* and ISPAK *(see Section 2.3.2)* were taken on board to develop draft legislation with the government concerning electronic crimes. The Senate Committee on Defence and Defence Production aims to create a national policy on cyber security. Part of the plan includes talks among the 8-member states of SAARC regarding acceptable norms of behavior in connection to cyber security[191] .

2.5 SUMMARY OF MAIN FINDINGS

The pillars of the state, inclusive of the military, all play a key role in internet governance and the future shape of cyberspace in Pakistan. While the PTA is charged with regulating the internet, and the FIA with online investigations, both institutions are almost entirely dependent on top-level control by the government and the military.

Further control by both institutions has been cemented in 2006 after the formation of the Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW), a shadowy regulatory body under the MoIT, whose members include government representatives and members of security agencies. Consequently, most ar-

186. Kugelman, M. (2012). Social media in Pakistan: catalyst for communication, not change. NOREF.
187. Hussain, C. F. (2013, January 2). Outcome of judicial activism. Retrieved September 29, 2013, from Dawn: http://beta.dawn.com/news/775678/outcome-of-judicial-activism
188. Ashraf, M. M. (2013, January 9). Judicial activism. Retrieved September 29, 2013, from Pakistan Today: http://www.pakistantoday.com.pk/2013/01/09/comment/columns/judicial-activism/
189. LHC bans Facebook while protests continue. (2010, May 19). Retrieved September 19, 2013, from The Express Tribune: http://tribune.com.pk/story/14370/lhc-bans-facebook-till-may-31/
190. Youtube ban: LHC directs govt to seek Google's view. (2013, April 27). Retrieved October 1, 2013, from The Express Tribune: http://tribune.com.pk/story/541127/youtube-ban-lhc-directs-govt-to-seek-googles-view/
191. APP. (2013, July 12). Senate committee proposes 7-point Action Plan for Cyber Secure Pakistan. Retrieved September 28, 2013, from Dawn: http://dawn.com/news/1023706/senate-committee-proposes-7-point-action-plan-for-cyber-secure-pakistan

bitrary blocks and filters since 2006 have focused on benefitting both parties, while radical religious groups have seen rapid, uninhibited growth in the online space, operating with impunity and forming a dangerous bloc that threatens cyberspace on many levels. The Fair Trial Act which was passed in 2013 has also given away further ground to the military in allowing online surveillance in an ill-defined, non-transparent manner.

ISPs have struggled with little success against the government, which held a virtual monopoly through the state-controlled PTCL till 2009. After PTCL's partial privatization and the decision to allowISPs to buy bandwidth from other third-party providers, a certain level of independence was attained, aided by ISPAK – a single body representing the ISPs. Unfortunately, existing legislation and regulations have left ISPs unable to defend their customers' basic rights. Little effort has been made by ISPs to change the existing environment to be conducive to a more democratic and open internet.

Unfortunately, the judiciary has yet to play an active role in correcting the increasing levels of state control of the internet. In fact, lawyers and judges have worked towards greater blocks and filters online in the past. As the IT and telecommunications industry grows and more businesses and local media move online, it is likely that the systems and legislation by which the internet is governed will come under greater scrutiny, criticism and hopefully, change.

3. CIVIL SOCIETY

3.1 CIVIL SOCIETY ACTIVE ON INTERNET ISSUES

Pakistan's civil society, while small in number, has played an active, albeit largely reactionary role on internet related issues, especially online censorship. Social media in particular has been leveraged by citizens to raise their voice against curbs on fundamental rights, to disseminate information and build a movement, to attract local and international attention– and resultant pressure – to an issue, and organize protests. From the ban on YouTube, Facebook and Twitter, to the ban on open VPNs, mobile phone service blackouts or attempted blockage of SMS words *(See section 1.1)*, online activists have criticised and in some cases, campaigned successfully against the state. At the same time, friction and divisions exist in the online community when sensitive topics like pornography and blasphemy are involved, with the largely conservative, religious majority and a highly active extremist minority supporting bans on such content.

Social media networks and sites that can host user-generated content (UGC) have been critical to civil society action. Facebook has 10 million Pakistani users[192]; Twitter is estimated to have 2 million users, while social media penetration of the country's total population is about 4%[193]. Pakistan also has a rapidly growing bloggers community with many key emerging influencers. More and more blogs enter the local blogosphere every day[194]. Blogspot.com is ranked among the top five visited sites by Pakistanis, while the top 20 include Facebook, YouTube, DailyMotion, Blogger.com, Wordpress.com, Pinterest and Twitter[195] ; all platforms featuring UGC and serving as spaces for civil society action. Additionally, bloggers have the support of local media organizations that run large blog sections or portals, including the Urdu-language daily Jang, Geo TV, English-language dailies The Express Tribune, Dawn and The News, all of whom feature in Alexa's top 100 list of websites visited by Pakistanis.

In terms of Facebook and Twitter, civil society has been active in engaging on internet governance and regulation. Facebook campaigns have consisted of the formation of Facebook groups, pages and viral shares either for, or against state-led action, while Twitter hashtags have been a defining campaign tool on the micro-blogging site. In many instances, activists and supporters unified under hashtags like #Stopcensoringpk[196] against the proposed national URL filtering system, #PTAbannedlist and #PTAbannedwords[197] against the SMS word filtration plan and #FbbanPK[198] against the 2010 ban on Facebook.

In the case of the national URL filtering system and the SMS word filtration plans, the ensuing social media uproar, resultant media coverage, online petitions and efforts of civil society organizations led to the PTA deciding against pursuing the projects, highlighting successful civil society pushback. Notably, Bolo Bhi, a not-for-profit organization based in Pakistan worked with other groups to convince five international companies that sell surveillance, filtering and blocking systems to publicly commit not to apply for Pakistan's URL filtering project[199]. Bolo Bhi Director Sana Saleem along with bloggers Dr Awab Alvi, Faisal Kapadia and others also took the government to court against its practise of blocking websites and the plan to have a national filtering system in place. The petitioners argued that the IT Ministry and the PTA were illegally blocking and censoring access to some websites and forums that criticised the workings of the state. They urged the court to direct the respondents to ensure that no website or content be blocked without prior notice and public objections should be invited before any such action is taken[200]. Another notable example was Bytes for All (B4A) - a human rights organization that announced it would challenge the validity of the SMS filter in court[201];

> "Friction and divisions exist in the online community when sensitive topics like pornography and blasphemy are involved, with the largely conservative, religious majority and a highly active extremist minority supporting bans on such content.

192. Nasir, S. (2013, September 25). Pakistan crosses 10 million facebook users. Retrieved September 25, 2013, from The Express Tribune: http://tribune.com.pk/story/609177/pakistan-crosses-10-million-facebook-users/
193. Teller, S. (2013, June 24). Pakistan Market Trends 2013: Online, Mobile, Social – Things Are About To Take Off. Retrieved September 25, 2013, from Ansr.io: http://ansr.io/blog/pakistan-market-trends-2013-online-mobile-social/
194. Shaukat, A. (2012, January 3). 'Number of blogs rose by 70% in 18 months'. Retrieved September 26, 2013, from The Express Tribune: http://tribune.com.pk/story/316042/blogocracy-tri-city-unconference-camp-held-in-lahore/
195. Top sites in Pakistan. (2013). Retrieved September 20, 2013, from Alexa: http://www.alexa.com/topsites/countries/PK
196. Twitter Search - #Stopcensoringpk. (2013, September 26). Retrieved September 26, 2013, from Twitter: https://twitter.com/search?q=%23Stopcensoringpk&src=hash
197. Twitter Search - #PTABannedWords. (2013, September 26). Retrieved September 26, 2013, from Twitter: https://twitter.com/search?q=%23PTABannedWords
198. Twitter Search - #FBbanPK. (2013, September 26). Retrieved September 26, 2013, from Twitter: https://twitter.com/search?q=%23FBbanPK&src=hash
199. Ribeiro, J. (2012, April 2). Groups Pressure Pakistan to Stop National Internet Monitoring Plan. Retrieved September 26, 2013, from PC World: http://www.pcworld.com/article/253005/groups_pressure_pakistan_to_stop_national_internet_monitoring_plan.html
200. Khurshid, J. (2012, April 18). PTA put on notice over Internet censorship. Retrieved September 27, 2013, from The News: http://www.thenews.com.pk/Todays-News-4-103573-PTA-put-on-notice-over-Internet-censorship
201. Moral Policing gets an Upgrade in Pakistan. (2011, November 18). Retrieved September 26, 2013, from Bytes For All: http://content.bytesforall.pk/moral_policing

part of the immense pressure put on the PTA that eventually issued a statement, saying, "PTA has received input from customers, government and other quarters on this issue. Therefore, implementation of previous PTA instructions [on SMS filter] has been withheld[202].

Since many politicians have a presence on Facebook and Twitter[203], most online protests quickly reach those in power. Because of this proximity, the concerns of online activists are at least heard, if not addressed instantly. Former interior minister Rehman Malik had interacted with Twitter users and made several important statements related to the internet[204] via his personal account, while current IT minister Anusha Rehman deactivated her Twitter profile[205] after she was heavily criticised for her policy decisions related to internet censorship.

In general, bloggers independently manage to draw local and foreign media attention to issues and increase pressure against internet censorship. There are however some blogs that specifically focus on internet issues including the advocacy-focused Don't Block The Blog[206] and the news-driven ProPakistani[207] .Following the blockage of Blogspot.com *(see section 1.1.2)*, a campaign was launched by prominent blogger Dr Awab Alvi and political humourist Omer Alvie under the banner of Don't Block The Blog (DBTB), which criticised the blanket ban on the blogging domain, creating a media stir which built pressure on the government.

Aside from large-scale online protests, marginalized, targeted groups such as Baloch activists, members of the persecuted Ahmadiyya community and members of the Shia community have used the internet not only as a medium to highlight issues they face, but as a means to voice protest against state censorship of their presence on cyberspace *(See section 1.1.2 and 1.1.3).*

While there are numerous positive examples of civil society action, the spread of hate-speech and extremism in Pakistan's online space is a growing, dangerous trend that threatens and often directly challenges civil society efforts to maintain a free, open internet *(see Section 2.3.4).*

In this environment, there are a number of civil society organizations and groups that work on internet-related issues. Bolo Bhi is a not-for-profit organization that has focused on advocacy, policy and research in the areas of gender rights, government transparency, internet access, digital security and privacy. Its team works on bridging the gap between rights advocates, policy makers, media and citizens[208]. The organisation has been at the forefront of civil society campaigns and protests over internet censorship. Bolo Bhi had written to the Canadian government[209], inquiring about internet filtering software Netsweeper's presence in Pakistan, circulated online petitions against the state's plan to implement a national-level URL filtering and blocking system[210] convinced five international companies that sell surveillance, filtering and blocking systems to commit to not apply for a URL filtering project[211] and its Director - Ferieha Aziz –was appointed amicus curiae in the YouTube ban case being heard at the Lahore High Court.

Another such organization is Bytes for All (B4A) - a human rights organization with a focus on ICTs. B4A works on raising debate on the relevance of ICTs for sustainable development, and strengthening human rights movements in the country. It also focuses on capacity building of human rights defenders regarding digital security, online safety and privacy. Working on multiple campaigns against internet censorship and surveillance in Pakistan, B4A has raised awareness about cyberspace issues, and policy advocacy from a civil liberties and human rights perspective[212]. The globally acclaimed Take Back the Tech Campaign[213] is the flagship of B4A; a program which focuses on the strategic use of ICTs by women to fight violence against women in Pakistan.

The case for the unblocking of YouTube, was led by B4A, who filed a petition in the Lahore High Court challenging the ban in January 2013.The organization also wrote a wrote an Allegation Letter – a specified UN mechanism – to the UN Office of the High Commissioner for Human Rights over the government's move to block websites in the run-up to the 2013 general elections[214]. Its research report prepared in conjunction with Citizen Lab uncovered that the government issuing technology procured from Canadian

202. Attaa, A. (2011, November 22). PTA Decides to Withdraw SMS Filtration Orders. Retrieved September 26, 2013, from ProPakistani: http://propakistani.pk/2011/11/22/pta-decides-to-withdraw-sms-filtration-orders/
203. Siddiqui, T. (2012, May 19). Parliamentarian twitterati. Retrieved September 26, 2013, from The Express Tribune: http://tribune.com.pk/story/381100/parliamentarian-twitterati/
204. Ashraf, G. (2013, January 24). Rehman Malik admits defeat in unblocking YouTube. Retrieved September 26, 2013, from The Express Tribune: http://tribune.com.pk/story/498553/rehman-malik-admits-defeat-in-getting-youtube-unblocked/
205. IT Minister's Twitter account deactivated amidst critique of policies. (2013, July 24). Retrieved September 26, 2013, from The Express Tribune: http://tribune.com.pk/story/581423/it-ministers-twitter-account-deactivated-amidst-critique-of-policies/
206. Don't Block The Blog. (n.d.). Retrieved September 26, 2013, from http://dbtb.org/
207. ProPakistani. (n.d.). Retrieved September 26, 2013, from ProPakistani: http://propakistani.pk/
208. About Us - Bolo Bhi. (n.d.). Retrieved September 26, 2013, from Bolo Bhi: http://bolobhi.org/about-us/
209. Canadian Government Responds To Netsweeper's Presence In Pakistan. (2013, September 9). Retrieved September 26, 2013, from Bolo Bhi: http://bolobhi.org/canadian-government-responds-netsweeper-pakistan/
210. Saleem, S. (n.d.). Pakistan: Stop The Firewall, Say No To Blanket Ban, Put an end to censorship. Retrieved September 26, 2013, from MoveOn Petitions: http://petitions.moveon.org/sign/pakistan-stop-the-firewall-2?r_by=1898072&source=c.tw
211. Ribeiro, J. (2012, April 2). Groups Pressure Pakistan to Stop National Internet Monitoring Plan. Retrieved September 26, 2013, from PC World: http://www.pcworld.com/article/253005/groups_pressure_pakistan_to_stop_national_internet_monitoring_plan.html
212. About Us - Bytes For All. (n.d.). Retrieved September 26, 2013, from Bytes For All: http://content.bytesforall.pk/about
213. About the campaign. (n.d.). Retrieved September 26, 2013, from TakeBackTheTech: https://www.takebackthetech.net/page/about-campaign
214. Ahmad, S. (2013, March 13). Letter of Allegation regarding the blocking of websites by the Government of Pakistan in the run-up to Pakistan's general elections. Retrieved September 26, 2013, from Bytes For All: http://content.bytesforall.pk/sites/default/files/Bytes%20for%20All%20and%20MLDI%20Letter%20of%20Allegation%20website%20blocking%20Pakistan.pdf

service provider Netsweeper to block websites *(see Section 1.1)*. B4A and Citizen Lab also highlighted the presence of a FinFisher Command and Control centre in Pakistani territory, hosted on a network owned by PTCL[215].

The Karachi-based civil society organization PeaceNiche has also fought against internet censorship, most notably in 2010 when the government blocked Facebook over blasphemous content. PeaceNiche along with other concerned activists organised a peaceful protest in Karachi to debate the ban on the social networking website. The protest organisers, under the banner of Defenders of Internet Freedom, asserted that the banning of sites was against people's rights and interests - an assertion that resulted in protests against the activists by members of a religio-political party[216]. Despite working in a sometimes hostile environment, PeaceNiche has focused on promoting democratic discourse and conflict resolution through intellectual and cultural engagement in the areas of arts and culture, science and technology, and advocacy[217].

Citizens For Free And Responsible Media (CFRM) – an online Facebook-based platform for those concerned about media freedom – formed during a successful internet campaign that led to the firing of TV show host Maya Khan for her vigilante-style morning show[218]. The CFRM has worked on a number of internet-related issues, such as calling upon the government to lift a ban on The Baloch Hal – an online publication that covers the crisis in Balochistan[219].

Civil society agitation and friction peaked over the blockage of YouTube in 2012-13. Online protests, blogs, petitions, social media campaigns and general outrage and debate over the ban on the video sharing website have been almost as consistent as the ban itself. The online community has been divided over the issue as it pertains to blasphemy, with many citizens in favour of the ban and limits on free speech.

3.2 CIVIL SOCIETY WHO COULD BE ACTIVATED

The online Pakistani community is small in terms of the overall population, and at times fragmented on key issues related to the internet, leaving a vacuum which can be filled by individuals and groups that have the power to influence public opinion or lead protests and campaigns. These non-political influencers and groups can be engaged to raise awareness and encourage action amongst the general public about internet-related issues.

Given that Pakistani society is heavily influenced by celebrity culture – both entertainment and sports – and by clerics and community leaders[220], identifying progressive influencers from these areas would have the most impact as a strategy for activating civil society on internet issues.

In recent years, a growing number of celebrities have joined social media platforms such as Twitter and Facebook. From actresses like Mahira Khan and Ayesha Omar to singers like Salman Ahmad, Atif Aslam and Ali Zafar, many members of the entertainment industry can be found online, actively engaging with their fast-growing online networks that already comprise of hundreds of thousands[221], or even millions[222]. Similarly, sports stars like cricketer Shahid Afridi and tennis star Aisamul Haq have the potential to reach thousands and trigger a snowball effect in a matter of minutes on any issue. Additionally, there are certain key journalists that have managed to create large online networks on both Facebook and Twitter who could, on an individual level, leverage their networks to create awareness and positive change.

> "Given that Pakistani society is heavily influenced by celebrity culture – both entertainment and sports – and by clerics and community leaders, identifying progressive influencers from these areas would have the most impact as a strategy for activating civil society on internet issues.

In the last few years, a new crop of young and enthusiastic filmmakers have surfaced with projects that have struck a chord with the public. Pakistan's maiden Oscar winner Sharmeen Obaid Chinoy, Mehreen Jabbar and director of the movie 'Waar', Bilal Lashari are just a few prominent names of such filmmakers who use social media to stay connected with their fans. Given that their work is directly impacted by censorship, this emerging community could potentially help spread awareness about the importance of internet freedom and mobilise followers for campaigning, while creating documentaries or visual support for such efforts.

215. Notorious spy technology found in Pakistan. (2013, January 5). Retrieved September 26, 2013, from Bytes For All: http://content.bytesforall.pk/node/99
216. Saleem, S. (2010, May 20). Conference on internet censorship ends on sour note. Retrieved September 26, 2013, from The Express Tribune: http://tribune.com.pk/story/14763/conference-on-internet-censorship-ends-on-sour-note/
217. PeaceNiche. (n.d.). Retrieved September 26, 2013, from PeaceNiche: http://www.peaceniche.org/
218. Haque, J. (2012, February 5). After Maya Khan, CFRM to hold Pakistan media accountable. Retrieved September 26, 2013, from The Express Tribune: http://tribune.com.pk/story/332333/after-maya-khan-cfrm-to-hold-pakistan-media-accountable/
219. Citizens for Free and Responsible Media statement on the media and Balochistan. (2012, February 21). Retrieved September 26, 2013, from Facebook: https://www.facebook.com/C4FRM/posts/349008258472523
220. Malik, I. H. (n.d.). Culture and Customs of Pakistan . Retrieved October 1, 2013, from Google Books: http://books.google.com.pk/books?id=GQTABKAGaVgC&pg=PA136&lpg=PA136&dq=pakistan+celebrity+culture&source=bl&ots=AtHLPGlyK3&sig=Pp5yt3Onl248b6ebhdmhLZAG5Xo&hl=en&sa=X&ei=_Jw0UrfIBuSs4ASaxIHoDA&ved=0CDkQ6AEwAjgK#v=onepage&q=pakistan%20celebrity%20culture&f=
221. Twitter Celebrities Statistics - Pakistan. (2013). Retrieved September 27, 2013, from Social Bakers: http://www.socialbakers.com/twitter/group/celebrities/country/pakistan/
222. Pakistan Facebook Statistics. (2013). Retrieved September 27, 2013, from Social Bakers: http://www.socialbakers.com/facebook-statistics/pakistan

The presence of religious leaders in the online space should not be ignored. In a highly conservative, Muslim-majority country like Pakistan, religious leaders command a strong following. Religious scholar Javed Ahmad Ghamidi and singer turned religious scholar Junaid Jamshed are among a few such personalities who use social networks to engage with their followers and represent a more progressive religious viewpoint. These opinion leaders can initiate debate over issues that are otherwise considered taboo, especially the blasphemy laws in relation to internet blocks and bans. Because of their knowledge of Islam, people are more likely to accept their views on religious matters.

Aside from focusing on individuals, non-governmental organisations that are present online can also be involved in campaigns to raise awareness regarding the importance of access to information, free speech and online security issues. NGOs working on issues such as women and minority rights, reproductive issues, rape, religious tolerance or other sensitive/taboo topics could address online privacy, data protection, harassment and the blasphemy laws. For such groups, uncensored and secure internet is critical to their work, and hence puts them at the fore when it comes to internet-related issues. Such NGOs can be mobilised to build up pressure in cases related to internet censorship, online privacy and other campaigns, in addition to lobbying for changes in legislation. These may include War Against Rape – an NGO working to provide services to survivors of sexual assault and rape[223], White Ribbon Campaign Pakistan – an NGO that engages men to reduce violation of women's rights[224] and Citizens for Democracy – an umbrella group working against the misuse and abuse of the blasphemy laws[225] to name just a few of the hundreds of NGOs that could form a powerful network.

3.3 SUMMARY OF MAIN FINDINGS

Civil society in Pakistan is at a nascent stage online, yet has already proven itself to be a powerful force capable of thwarting government plans to control the internet, as well a community capable of organizing and leading protests – both online and on-ground – to push back against state control and interference.

While small in number, civil society members and activists are supported by a handful of non-profits and NGOS that work specifically on internet-related issues. These organizations have aided in enhancing awareness, providing structure and actionable points to protests and taking direct action such as court petitions.

The unexplored potential of civil society is largely dependent on whether key influencers in the online space – celebrities, religious leaders and NGOs in particular – can be engaged to form a more cohesive and powerful community. The great challenge for civil society is the rising tide of extremism in the online space, whose messages resonate with the conservative, religious majority in opposition to free, open and safe internet in Pakistan.

223. Introduction - WAR. (2013). Retrieved September 27, 2013, from War Against Rape: http://www.war.org.pk/index.php?id=1
224. About Us - White Ribbon. (2013). Retrieved September 27, 2013, from White Ribbon: http://www.whiteribbon.org.pk/page_id2/vision-and-mission/
225. About - citizensfordemocracy. (n.d.). Retrieved September 27, 2013, from Citizens For Democracy: http://citizensfordemocracy.wordpress.com/about/

ABOUT BYTES FOR ALL, PAKISTAN

Bytes for All (B4A), Pakistan is a human rights organization with a focus on Information and Communication Technologies (ICTs). It experiments and organizes debate on the relevance of ICTs for sustainable development and strengthening human rights movements in the country.

At the forefront of Internet Rights movement and struggle for the democracy, B4A focuses on capacity building of human rights defenders on their digital security, online safety & privacy. Working on different important campaigns particularly against Internet censorship and surveillance in Pakistan, B4A continues to work on cyberspace issues, awareness raising and policy advocacy from civil liberties & human rights perspective. Globally acclaimed Take Back The Tech Campaign is the flagship of Bytes for All, which focuses on strategic use of ICTs by the women and girls to fight violence against women in Pakistan.

B4A's field projects focus on:

i. Strategic use of ICTs for women's empowerment and combating violence against women;
ii. Youth & peace building in South Asia region
iii. Online Freedom of Expression;
iv. Privacy Rights in Pakistan;
v. Digital Security for Human Rights Defenders;
vi. Open Governance;
vii. Greening IT;
viii. Internet & Human Rights;
ix. Global Information Society Watch;
x. Innovation for Development; and
xi. Internet Governance.

For its work, B4A partners and collaborates with different civil society organizations. B4A's staff team is totally committed towards civil liberties in Pakistan.

B4A is a legally registered entity in Pakistan since 2009 and its organizational bank account is operated by Barclays Bank in Islamabad, Pakistan.

Bytes for All, Pakistan
Tel. +92 (51) 2110494-5,
House 273, Street 17, F - 10/2
info@bytesforall.pk
Islamabad, Pakistan
www.bytesforall.pk