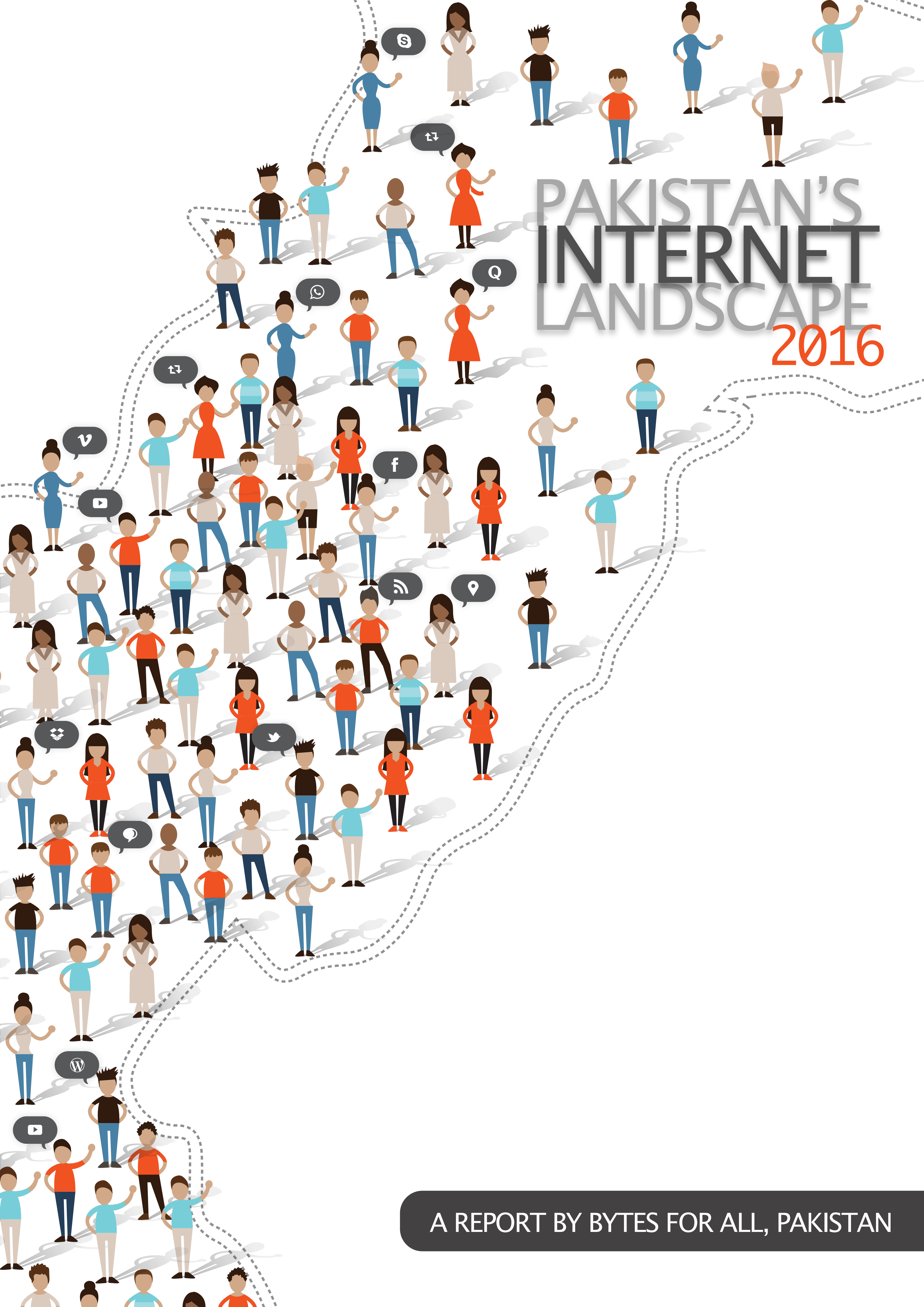


# PAKISTAN'S INTERNET LANDSCAPE 2016

A REPORT BY BYTES FOR ALL, PAKISTAN

# PAKISTAN'S INTERNET LANDSCAPE 2016

Written by
Jahanzaib Haque

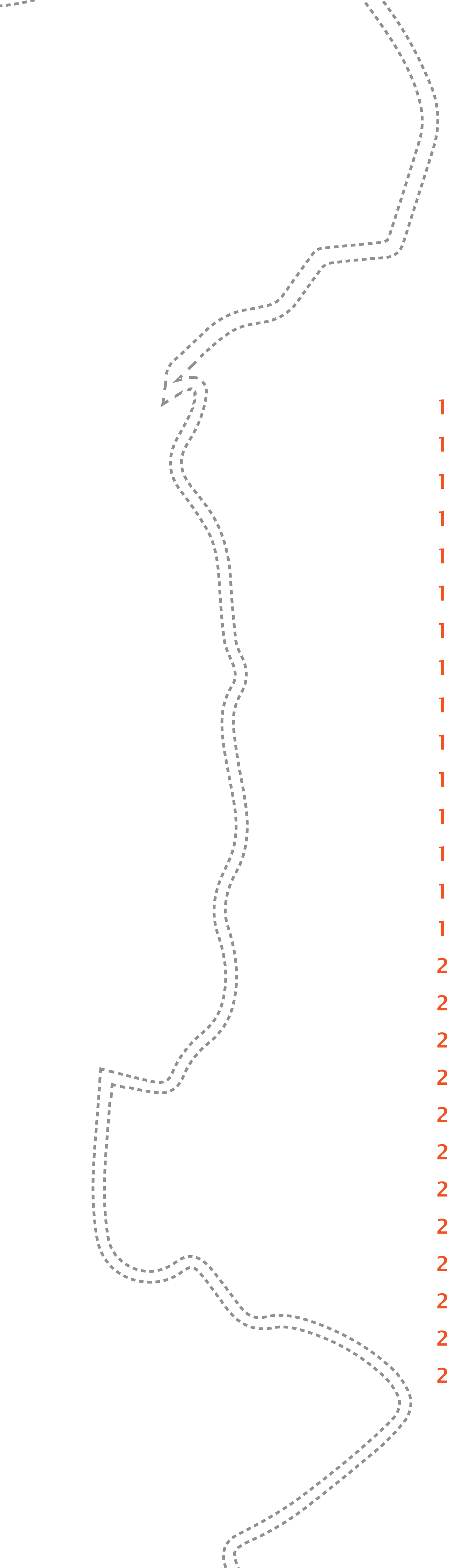
Assistant Researcher
Hufsa Chaudhry

Design by
Rabeea Arif & Sara Nisar

JULY, 2016

This research has been produced by Bytes for All, Pakistan in collaboration with Global Partners Digital.

# TABLE OF CONTENTS



# PREFACE

Many changes have taken place since the launch of the Pakistan Internet Landscape Report (ILR) 2013 – many have been unexpected, many troubling.

While access and speed of the internet has increased, the country still remains far behind the rest of the world. Increased access has also come with increased state control over the internet in the form of continuing censorship, greater monitoring of online activity and dangerous legislation that is open to abuse, trampling on basic rights of citizens while meting out harsh punishments.

This new report continues the documentation of the country's internet landscape from a critical, human rights perspective.

The methodology used for compiling this report is a combination of secondary sources including news reports, investigative studies, survey and other research. As such, the document should be read as part historical record and part analysis.

The aim is to provide reference points for meaningful dialogue on the issues highlighted, with the hope that progressive policies, and most importantly, a progressive mindset emerges to guide Pakistan's online future.

# EXECUTIVE SUMMARY

Pakistan's online journey from 2014 to 2016 has been greatly shaped with the rapid jump in internet penetration following the introduction of 3G/4G to the country. While still ranked among the five least connected countries globally, as of February 2016, mobile internet users (3G/4G) stood at 26.19 million, while as of January 2016, there were 29.32 million broadband subscribers (inclusive of mobile broadband). Unfortunately, the digital divide has persisted, with access being quite rigidly determined by whether an individual lives in an urban/rural setting; age; education; income; owning a smartphone. (See Section 1.0 for details)

26.19 million
mobile internet users

29.32 million
broadband subscribers

With regards to blocking and filtering of content, The Freedom of the Internet 2015 report published annually by Freedom House gave Pakistan its lowest status of 'Not Free' due to consistent online censorship. Such censorship has been carried out by the Pakistan Telecommunication Authority (PTA), given the dismantling of the controversial Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW). The regulatory body has issued multiple orders for blocking access to parts of the internet in the last two years. The most prominent ban order came in January 2016, where ISPs were ordered to block over 400,000 'pornographic' sites following an order of the Supreme Court.

The last two years have also seen a new, troubling trend – greater coordination between the state and internet companies such as Google, Facebook and Twitter, where the companies have complied, to varying degrees, with government orders to block access to content, provide private information of users or in the case of Google, set up a localized version of YouTube to allow for the lifting of the years-long ban of the site, at the price of restricting 'objectionable content' in Pakistan. (See Section 1.1 and 1.1.1. for details)

A small but steady stream of online 'blasphemy' cases indicate the coming years will see large growth in blasphemy-related censorship. However, the more worrying aspect of this trend is that most result in real world violence and arrests of individuals embroiled in such cases. At its most extreme, three female members of the minority Ahmadi community were killed by an enraged mob for an alleged blasphemous Facebook post by an Ahmadi youth from the same village.

> "The coming years will see large growth in blasphemy-related censorship"

Making matters worse, enraged citizens, those with vested interests, and often times both groups have used cyberspace to amplify blasphemy allegations emanating from other mediums, such as the case of singer-turned-preacher Junaid Jamshed who had to flee the country after a video of one of his religious sermons – deemed blasphemous – went viral online. (See Section 1.1.2. for details)

New dimensions have also emerged in the ongoing, decades-long blocking of content deemed anti-state. In 2015, the Lahore High Court ordered the Pakistan Electronic Media Regulatory Authority (Pemra) and the Press Council of Pakistan (PCP) to block all speeches and visuals of MQM Chief Altaf Hussain on both print and electronic media. The order came after the MQM Chief made alleged remarks against state institutions, including the army and Rangers, during a speech that was distributed widely on all mediums. The directive was followed by all media groups and extended to the digital space as well.

With regards to non-state actors i.e. terrorists and banned outfits, very little has been done to effectively block their anti-state propaganda online. Websites and social media accounts/pages are sporadically removed, but reappear again under different names, different domains.

In another new development, traditional media have been targeted in threatening social media campaigns that create an atmosphere of fear, leading to self-censorship of any criticism of the state. The campaigns, generally carried out on Twitter, have almost exclusively focused on framing the media person/group as 'anti-Pakistan' and/or 'anti-Islam'. (See Section 1.1.3. for details)

> "Traditional media has been targeted in threatening
> threatening social media campaigns
> that create an atmosphere of fear"

In order to justify state action, the last two years have seen one harsh and highly controversial piece of legislation, the Protection of Pakistan Act, 2014 (PPA) come into play, while another draft legislation, the equally controversial and criticized Prevention of Electronic Crimes Bill (PECB) come forward as a response to increased acts of terror in the country.

The PPA, which has been made law, includes within its Schedule of offences, "committed with the purpose of waging war or insurrection against Pakistan or threatening the security of Pakistan" (xiv) cyber-crimes, internet offences and other offences related to information technology which facilitates any offence under this Act. The addition of section xiv, with no further definition of the terms used therein allow for all parts of the highly controversial act to apply to cyberspace.

The PECB draft bill has been called a 'key pillar' of National Action Plan by the government - a multi-pronged strategy launched in 2015 following the attack on the Peshawar Army Public

School that killed over 144 people, mostly children. NAP, has redefined Pakistan's policies including the internet in profound ways, shifting focus heavily towards anti-terrorism efforts.

Consequently, the draft bill of the PECB passed by the National Assembly proposes 14-year imprisonment or Rs50 million fine or both for those found guilty of cyber terrorism. The bill's language is loose enough to: criminalize whistleblowing, allow for the blocking of many forms of content including satire; criminalize the use of VPNs that allow for private, encrypted browsing; criminalize communication that praises any person simply accused of a crime, not convicted. Each of the 'crimes' carry heavy penalties and even imprisonment.

14 years
possible imprisonment
for 'cyber terrorism'

Once passed by Senate, critics fear the bill will be misused by the state to consolidate control of the internet and target ordinary citizens. (See Section 1.2. for details)

Regarding surveillance, a number of revelations this year have established a clearer picture of the government's online surveillance efforts. Most critically, a Privacy International report uncovered that the government obtained 'cyber security' surveillance tools from multiple international companies that enable high-level spying. This was partly made possible by funding from foreign governments as part of counter-insurgency efforts. According to the report, massive surveillance has been ongoing since 2005. A leak of emails from Italian security firm Hacking Team further established that Pakistani contractors had been working to procure invasive online spying tools.

Aside from technical solutions, the state has also built its relationship with Facebook, where millions of Pakistani users are active, to gain access to private data of some accounts.

These efforts are being legitimized by the state by the passing of laws that justify invasion of privacy in the name of countering terrorism, namely the PPA and the upcoming PECB. (see Section 1.2.)

# 1.0 ACCESS TO INTERNET

In the Internet Landscape Report 2013 (ILR), it was noted that there were many different estimates and wide ranges for internet penetration in Pakistan, ranging from 10%[1] to 16%[2] of the overall population. This wide range continued to persist in 2014-16, with numbers ranging from 10.8% to 17% internet penetration.

According to 2015 ITU statistics, internet penetration in Pakistan stood at 13.8% of the population in 2014, against the average penetration of 33.8% in Asia. The Asia region average further climbed to 36.9% by 2015[3]. For the same 2014 period, the CIA World Factbook put internet penetration estimates at 10.8%[4].

A 2016 PEW report noted that Pakistan's internet penetration stood at a low 15% in spring 2015[5]. A 2016 World Bank report noted that Pakistan was among the five least connected countries globally. Only 17% of the population of 200 million was found to be online.

> "A 2016 World Bank report noted that Pakistan was among the five least-connected countries globally"

The official Pakistan Telecommunication Authority (PTA) telecom indicators show a more detailed picture in light of 3G/4G internet access after the introduction of the networks in Pakistan[6]. As of February 2016, mobile internet users (3G/4G) stood at 26.19 million, while as of January 2016, there were 29.32 million broadband subscribers (inclusive of mobile broadband). Even considering overlap of mobile and broadband users, the growth through 3G/4G has been rapid. In the 2013 Internet Landscape report, broadband subscriptions,

[1] ***Percentage of individuals using the Internet.*** (n.d.). Retrieved on May 14, 2016, from International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Individuals_Internet_2000-2014.xls

[2] ***30m internet users in Pakistan, half on mobile: Report.*** (2013, June 24). Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobile-report/

[3] ***TU Statistics 2015*** Retrieved on May 14, 2016, from the International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[4] ***The World Factbook – Pakistan*** Retrieved on May 14, 2016 from the Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/pk.html

[5] Poushter, J. (2016, February 22). ***Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*** Retrieved on July 3, 2016, from Pew: http://www.pewglobal.org/files/2016/02/pew_research_center_global_technology_report_final_february_22__2016.pdf

[6] Anis, K. (2014, April 23). ***Pakistan Raises $1.13 Billion in Auction for 3G, 4G Spectrum*** Retrieved on July 3, 2016, from Bloomberg: http://www.bloomberg.com/news/articles/2014-04-23/pakistan-raises-1-13-billion-in-auction-for-3g-4g-spectrum

comprised largely of DSL, WiMax and EvDo stand at a low 2.6 million[7]. This would indicate a ten-fold growth in subscribers over three years.

With more than 90% of citizens living in areas that have mobile coverage[8], the potential for far greater internet penetration with the proliferation of cheap smart phones and cheaper 3G/4G packages remains high. This is bolstered by the fact that, according to a report by the Pakistan Demographic and Health Survey (PDHS), 94.7% of the urban population owns a mobile phone, as do 83% of those in rural areas[9].

97% of urban population
owns a mobile phone

According to the Internet Service Providers Association of Pakistan (ISPAK) – a platform representing ISPs in the country (see Section 2.3.2), the number of operational Internet service providers (ISPs) has remained at 50, as indicated in 2013 as well[10]. Undersea cables distribution remains the same, with three with PTCL – SMW3, SMW4 and IMEWE – and one with TransWorld International. The domestic fiber backbones now include PTCL, Wateen, Mobilink and Multinet.

One of the major challenges noted in the ILR 2013, the digital divide between the haves and the have-nots has persisted with little change to be seen. According to the 2016 PEW report, with 15% total internet penetration, younger people (18-34 bracket) having 20% penetration in Pakistan[11]. The report also uncovered a vast digital divide in access between those who had more education (33% penetration) to those with less (6%). Income was also a major factor, with the higher income group having 20% internet penetration as compare to 8% in the lower income group. With regards to ownership of smart phones, another indicator of meaningful internet access, the report found that only 11% of Pakistani respondents owned a smart phone. Again, those in the younger age bracket, with higher education and higher income had far great percentages of smart phone owners than their counterparts.

These findings tie in to earlier reports that a majority of Pakistan's internet users are located in the urban centres, which comprise only 36% of the total population[12]. A BBC survey in

[7] ***Telecom Indicators*** Retrieved on May 14, 2016, from the Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?Itemid=599

[8] ***The World Factbook – Pakistan*** Retrieved on May 14, 2016 from the Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/pk.html

[9] ***Pakistan Demographic and Health Survey 2012-2013*** Retrieved on May 30, 2016, from The DHS Program: http://dhsprogram.com/pubs/pdf/FR290/FR290.pdf

[10] ***ISPAK*** Retrieved on May 14, 2016, from the Internet Service Providers Association of Pakistan: http://www.ispak.pk/

[11] Poushter, J. (2016, February 22). ***Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*** Retrieved on July 3, 2016, from Pew: http://www.pewglobal.org/files/2016/02/pew_research_center_global_technology_report_final_february_22__2016.pdf

[12] ***The World Factbook – Pakistan*** Retrieved on May 14, 2016 from the Central Intelligence Agency: https://www.cia.gov/library/publications/the-world-factbook/geos/pk.html

2008 had found that 34% of the urban population said they had access to the internet, as compared to only 3% of the rural population[13].

As indicated in ILR 2013, a host of factors continue to hold back the spread of the internet, specifically to rural areas and low income households. The Freedom of the Internet 2015 report released annually by Freedom House found a host of factors holding Pakistan back: "Low literacy, difficult economic conditions, and cultural resistance have limited the proliferation of ICTs in Pakistan. While the cost of internet use has fallen considerably in the last few years, with prices around US$12 a month for a broadband package in 2015, access remains out of reach for the majority of people in Pakistan. Though ICT usage by girls and women in Pakistan is gradually increasing, online harassment unfortunately discourages greater utilization of ICTs by women, especially those under 30.[14]"

With regards to cultural resistance, a Pew Global Attitudes survey of 32 countries published in 2015 found that a low 20% of Pakistanis felt the internet was a good influence when answering, "Has the increasing use of the internet had a good influence, a bad influence, or no influence at all on morality?"[15] While 31% felt it had a bad influence, the majority 43% indicated they did not know/refused to answer the question. In the same survey, Pakistani respondents ranked among the lowest of those surveyed with regards to whether the internet was a good influence on politics, economy, education and personal relationships.

only 20% of Pakistanis
felt the Internet was a good influence
(2015 PEW survey)

[13] ***Internet in Pakistan.*** (n.d.). Retrieved on May 14, 2016, from Audiencescapes: http://www.audiencescapes.org/country-profiles-pakistan-country-overview-internet-research-statistics

[14] ***Pakistan country report 2015*** Retrieved on May 14, 2016, from Freedom On The Net: https://freedomhouse.org/report/freedom-net/2015/pakistan

[15] ***Internet seen as positive influence on education but negative on morality in emerging and developing nations*** Retrieved on May 30, 2016, from Pew: http://www.pewglobal.org/2015/03/19/internet-seen-as-positive-influence-on-education-but-negative-influence-on-morality-in-emerging-and-developing-nations/

# 1.1 BLOCKING & FILTERING

Censorship of the internet has continued into 2016 in Pakistan, with focus remaining on content deemed pornographic, blasphemous or anti-state.

The Freedom of the Internet 2015 report published annually by Freedom House gave Pakistan its lowest status of 'Not Free'. The report notes: "Extralegal pressure on publishers and content producers by the state or other actors to remove content is not unknown in Pakistan, but frequently goes unreported." It highlighted that social media/ICT apps had been blocked, as had political/social content, and bloggers/ICT users were arrested[16].

The PTA has continued to take action against and ordered ISPs to block access to parts of cyberspace, although as admitted in a recent report, the body expressed helplessness in blocking content. The report stated, "Technically, 100 per cent blocking of websites containing offensive material is not possible because numerous proxy sites are being built every single day. In addition, lots of new websites are also being made and uploaded on a daily basis. Virtual Private Networks (VPNs) and proxies are also used to access these sites, despite blocking." In a rare admission, the report stated that blocking sites at such a large scale would lead to "deteriorating internet quality in terms of speed and availability". Despite the apparent challenges faced by the PTA, the regulatory body confirmed having blocked 84,000 sites containing 'objectionable' content, and a total of 200,000 links to 'obscene material' in 2012 [17].

> "Mass blocking of sites will lead to "deteriorating internet quality in terms of speed and availability" PTA

In January this year, the PTA announced that it had ordered ISPs to block over 400,000 adult websites at the domain level following an order of the Supreme Court that asked the body to take steps against, "obscenity and pornography that has an imminent role to corrupt and vitiate the youth of Pakistan". As stated in a news report, ISP officials said such an exercise would be 'gigantic and costly'. ISPs are required to carry out blocking directives issued by the PTA, or face license suspensions for failure to respond[18].

[16] ***Pakistan country report 2015*** Retrieved on May 14, 2016, from Freedom On The Net: https://freedomhouse.org/report/freedom-net/2015/pakistan

[17] ***PTI.*** (2012, October 8). Pakistan blocks 20,000 websites Retrieved on May 14, 2016, from The Hindu: http://www.thehindu.com/news/international/pakistan-blocks-20000-websites/article3977440.ece

[18] Baloch, F. (2016, January 26). ***Pakistan to block over 400,000 porn websites.*** Retrieved on May 14, 2016 from The Express Tribune: http://tribune.com.pk/story/1034224/objectionable-content-isps-ordered-to-block-400000-pornographic-websites/

These numbers are a big jump up from those reported in ILR 2013, where reported estimates ranged from 20,000 to 40,000 blocked sites. As noted before, past and current numbers of blocked sites may be far lower than actual figures, given the non-transparent, arbitrary process by which content is blocked. 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.

In 2014, Twitter blocked 'blasphemous' and 'unethical' content including tweets and some Twitter accounts in Pakistan on the request of the government – a decision that was reversed shortly after[19]. Similarly, Facebook also blocks content on the state's request, the most high-profile case being the block of rock band Laal's Facebook page in 2014. The government later withdrew the decision following public outcry online. At the time, a Facebook spokesperson said the request from the PTA had been complied with as the company's policy was to adhere to local laws; no explanation was given for which law the page was blocked under[20].

In another high-profile case on Pakistan Day, March 23 2015, Pakistani internet users were unable to access Wordpress. As cited in a news report, "The website was inaccessible on several major internet service providers...but there was no official word from the Pakistan Telecommunication Authority (PTA) on whether the ban was official or not[21]."

In a major development since ILR 2013, after the Islamabad High Court barred the controversial Inter-Ministerial Committee for the Evaluation of Web sites (IMCEW) from playing any role in website content management, the shadowy committee was disbanded by Prime Minister Nawaz Sharif in March 2015, with powers being transferred to the PTA. The IMCEW had been primarily responsible for determining what online content was to be blocked over many years. The committee had comprised representatives of ministries of interior, cabinet, information and broadcasting and security agencies. The names of the members of this committee were never made public, nor were any details of their decision making.

According to one news report, the PTA was directed to establish a mechanism for web content management" but at the same time, ordered to safeguard fundamental rights of citizens while "the participation of relevant stakeholders in evaluation of complaints and decisions thereon will be ensured. A mechanism for redressal of grievances for affected users will also be provided. To ensure effectiveness of the content management system, PTA will also adequately strengthen its web monitoring cell." It is however unclear to what extent the PTA follows the directives, given a lack of transparency in its content blocking operations[22].

[19] Elder, J. (2014, June 17). ***Twitter restores content blocked at Pakistan's request*** Retrieved on May 30, 2016, from The Wall Street Journal: http://blogs.wsj.com/digits/2014/06/17/twitter-restores-content-blocked-at-pakistans-request/

[20] Walsh, D., Masood, S. (2014, June 6). ***Facebook under fire for temporarily blocking pages in Pakistan*** Retrieved on May 30, 2016 from The New York Times: http://www.nytimes.com/2014/06/07/world/asia/pakistan-facebook-blocked-users-from-political-pages-and-outspoken-rock-band-laal-against-taliban-.html?_r=0

[21] ***Blogging website Wordpress blocked*** (2015, March 23). Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1171304

[22] Haider, M. (2015, March 21). ***PTA given powers for content management on internet*** Retrieved on May 14, 2016, from The News: http://www.thenews.com.pk/print/30534-pta-given-powers-for-content-management-on-internet

One positive development in 2016 was the lifting of the years-long ban on video-hosting website YouTube. The site had been blocked in 2012 after Pakistan witnessed violent protests following the release of the trailer of a blasphemous film, ‘Innocence of Muslims’. The end of the ban came with Google setting up a localised version of YouTube and, according to a PTA official, an agreement that “objectionable content will be restricted in Pakistan. It has assured that, in the future, content can be restricted at the request of the government of Pakistan.” This agreement has been criticised by local digital activists and rights groups for the possibility that it may empower the government to censor content on the website.

> “Objectionable content [on YouTube]
> will be restricted in Pakistan” PTA

Agreements between the government and social network Facebook also drew similar criticism, as in 2014, the annual Facebook ‘Government Requests Report’ showed a 10-fold increase in data/content restrictions carried out by the company under the government’s request[23]. A Facebook statement on the report said, “We restricted access in Pakistan to a number of pieces of content primarily reported by the Pakistan Telecommunication Authority (PTA) and the Ministry of Information Technology under local laws prohibiting blasphemy and criticism of the state.”

In the first six months of 2015, the Facebook report showed 192 government requests and 275 user accounts requests, with Facebook complying 58.33% of the time – another big leap up from 2014. However, a large leap was also seen in the last six months of 2015, where 471 requests were made, 706 accounts requested, with Facebook complying a much higher 66.45% of the time[24].

Along with coordination with social media giants come worrying real world consequences. In 2015, a member of the Shia committee was jailed by an anti-terrorism court for posting alleged ‘sectarian hate speech’ on social media, a move that was condemned by human rights activists for coming under terrorist activity[25]. The same report cited that on that day, a man in Faisalabad was arrested for airing ‘hate material’ on social media. This too came under the anti-terrorism act. And in July, according to the Dawn report, a local prayer leader was similarly booked for posting ‘hate comments’ on Facebook. In each case, heavy penalties and prison time were meted out given that the anti-terrorism act was imposed.

[23] ***Pakistan government requests for data*** 1H14 Retrieved on May 30, 2016, from Facebook: https://govtrequests.facebook.com/country/Pakistan/2014-H1/

[24] ***Pakistan government requests for data*** 2H15 Retrieved on May 30, 2016, from Facebook: https://govtrequests.facebook.com/country/Pakistan/2015-H2/

[25] (AFP, APP, & Gabol, ***Pakistani Shia man jailed for 13 years for Facebook 'hate speech'***, 2015)

Unfortunately, it seems there is some public support for the government's policies in favor of online censorship. According to a Pew Global Attitudes survey on freedom on the Internet in emerging and developing nations 2015, most Pakistanis show little support for uncensored access to the internet. Pakistan had one of the lowest levels of public support of 38 countries surveyed when asked if it was important that people have access to the internet without government censorship[26]. Only 25% of Pakistani respondents supported a free internet.

only 25% of Pakistani respondents
supported a free internet
(2015 PEW survey)

## 1.1.1 PORNOGRAPHY

Pornographic content has been blocked for years under the broad term 'obscene' and similar vague definitions in the Pakistan Telecommunications (re-organisation) Act, 1996 (see Section 1.2).

In January 2016, the PTA ordered ISPs to block over 400,000 adult websites at the domain level –following an order of the Supreme Court that asked the body to take steps against, "obscenity and pornography that has an imminent role to corrupt and vitiate the youth of Pakistan". As stated in a news report, ISP officials said such an exercise would be 'gigantic and costly'. ISPs are required to carry out blocking directives issued by the PTA, or face license suspensions for failure to respond[27].

This ban order is the latest, and one of the largest, for blockage of porn sites in Pakistan's history. As in the past, no public list was made available of which over 400,000 sites were to be blocked. An investigation into the list retrieved through ISP sources uncovered hundreds of non-pornographic or offensive sites were in the list, along with thousands of others that were unpurchased domains hosting no content, pointing towards a flawed process that restricted access to information[28].

This lack of transparency regarding what is blocked, and the often inexplicable inclusion of non-offensive sites continues a trend that has lasted over two decades (see ILR 2013 for details).

[26] Wike, R., Simmons, K. (2015, November 18). ***Global support for principle of free expression, but opposition to some forms of speech*** Retrieved on May 30, 2016, from Pew: http://www.pewglobal.org/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/

[27] Baloch, F. (2016, January 26). ***Pakistan to block over 400,000 porn websites*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/1034224/objectionable-content-isps-ordered-to-block-400000-pornographic-websites/

[28] Haque, J. (2016, May 25). ***Rudderless: Pakistan's impossible attempt to block 400,000 porn sites continues*** Retrieved on May 30, 2016, from Dawn: http://www.dawn.com/news/1260172/rudderless-pakistans-impossible-attempt-to-block-400000-porn-sites-continues

## 1.1.2 BLASPHEMY

Blocking of websites for hosting blasphemous content has remained a priority for the state, continuing a trend that began in 2003 (see ILR 2013 for more details on the blasphemy laws), one that has seen some of the largest sites in the world – Facebook, Blogspot, Twitter, YouTube – banned for periods as short as days and in the case of YouTube, years. Additionally, blasphemous content online has increasingly led to real-world consequences against citizens.

In 2014, a Christian man was arrested and booked for blasphemy for his blog posts that allegedly used derogatory language against the Holy Prophet (PBUH). According to a report, "a man posted a comment on the website of a private TV channel and alleged that the accused was committing blasphemy in his blogs" following which a case had been registered against the suspect[29].

In Sheikhupura this year, a man was arrested for posting 'blasphemous' content on social media, although investigations showed that the messages were posted over a year ago by another individual who had left the country[30].

The Freedom on the Net 2015 report allegations of blasphemy related to online content show an upward trend in Pakistan[31]. It says: "Blasphemy charges related to online content continue to restrict the environment for ordinary internet users."

The online space has also become an amplifier for alleged blasphemy in other mediums. A blasphemy case was registered against singer-turned-preacher Junaid Jamshed in 2014 after a video of one of his religious sermons went viral online. The video caused a social media uproar with accusations that Jamshed had blasphemed while preaching. Jamshed fled Pakistan to avoid arrest, and later released an online video apologising for his remarks[32].

Very similarly, a blasphemy case was registered against Jang Media Group owner Mir Shakeel-ur-Rehman after a clip of an alleged blasphemous TV show episode went viral online, followed by a campaign on social media and on TV by a rival media group. The clip showed a celebratory dance performed on a song about the Holy Prophet's (PBUH) daughter[33]. In both the case of Junaid Jamshed and Mir Shakeel-ur-Rehman, no arrests were made, with Jamshed eventually returning to Pakistan.

[29] ***Man held over blasphemy allegation*** (2014, November 15). Retrieved April 29, 2016, from Dawn: http://www.dawn.com/news/1144655

[30] ***Man arrested on blasphemy charge*** (2016, May 26). Retrieved on May 30, 2016, from Dawn: http://www.dawn.com/news/1260754/man-arrested-on-blasphemy-charge

[31] ***Pakistan country report 2015*** Retrieved on May 30, 2016, from Freedom On The Net: https://freedomhouse.org/report/freedom-net/2015/pakistan

[32] ***Junaid Jamshed booked for blasphemy.*** (2014, December 3). Retrieved on April 29, 2016, from Dawn: http://www.dawn.com/news/1148479

[33] ***Pakistan TV mogul gets 26 years' jail for blasphemy.*** (2014, November 26). Retrieved on April 29, 2016, from Reuters: http://www.reuters.com/article/pakistan-media-idUSL3N0TG27R20141126

Another instance that shows the vulnerability of social media users to allegations of blasphemy is that of a Facebook group, 'All Pakistan Girls', against which a petition was filed after it was alleged to have shared blasphemous material on the social network. The FIA were ordered to investigate the matter by an additional district and sessions judge. There was no reported follow-up to the case however[34]. Three female members of the minority Ahmadi community were also killed by an enraged mob for an alleged blasphemous Facebook post by an Ahmadi youth from the same village[35].

> "Three female members of the Ahmadi community were killed for an alleged blasphemous Facebook post"

This disturbing trend suggests that as internet penetration increases, allegations of online blasphemy and resultant arrests and/or violence will increase as well, given the lack of response by the government. The PTA has set up a number of methods for the reporting of blasphemous URLS[36].

As stated in a 2015 study 'Blasphemy in the Digital Age' conducted by local NGO Digital Rights Foundation, "The state's willingness as well as ability to curb vigilante violence is seriously lacking. This becomes particularly severe in the digital age, since false accusations about a subject as evocative and sensitive as blasphemy can be spread within seconds – leaving the accused deeply vulnerable.

## 1.1.3 ANTI-STATE

'Anti-state' content has been blocked or ordered to be blocked on several known occasions since ILR 2013, along with a new trend of threatening social media campaigns against local media groups to apply pressure for the removal of content, or to prompt self-censorship in future. Most of the focus has shifted to preventing mainstream access to such content, while previously the focus had remained on blocking niche/fringe elements online such as sites run by Baloch separatists[37], or individual pieces of content that were critical of the state or politicians[38].

[34] ***Cyber crime: FIA director asked to investigate alleged blasphemy.*** (2014, June 11). Retrieved on April 29, 2016, from The Express Tribune: http://tribune.com.pk/story/720124/cyber-crime-fia-director-asked-to-investigate-alleged-blasphemy/

[35] ***Mob attack over alleged blasphemy: Three Ahmadis killed in Gujranwala.*** (2014, July 28). Retrieved on April 29, 2016, from Dawn: http://www.dawn.com/news/1122143

[36] ***Report blasphemous URL*** Retrieved on April 29, 2016, from the Pakistan Telecommunication Authority: http://www.pta.gov.pk/index.php?Itemid=785

[37] ***Waking up to the war in Balochistan.*** (2012, February 29). Retrieved on May 14, 2016, from BBC News: http://www.bbc.co.uk/news/world-asia-17029159

[38] James, M. (2010, February 7). ***'Shut Up'? Pakistan President's Outburst Scrubbed From 'Net.*** Retrieved on May 14, 2016, from ABC News: http://abcnews.go.com/blogs/headlines/2010/02/shut-up-pakistan-presidents-outburst-scrubbed-from-net/

The most prominent case of censorship was in 2015, when the Lahore High Court ordered the Pakistan Electronic Media Regulatory Authority (Pemra) and the Press Council of Pakistan (PCP) to block out all speeches and visuals of MQM Chief Altaf Hussain on both print and electronic media. The order came after the MQM Chief made alleged remarks against state institutions, including the army and Rangers, during a speech that was distributed widely on all mediums. The directive remains in place and has been followed by media groups in the digital space as well[39].

One of the more problematic trends has been Facebook's cooperation with the government in blocking anti-state content. In 2014, Facebook blocked Pakistan users from accessing local rock band Laal's Facebook page following a request from the government. The band is known for its critical, outspoken stance of state policies. Numerous other left-leaning pages were also made inaccessible at the same time. After a media outcry, the government reversed its decision and Facebook made the Laal page accessible[40].

> "One of the more problematic trends has been Facebook's cooperation with the government in blocking the content"

Critics have called out the state for focusing on blocking legitimate political dissent, while allowing non-state actors such as terrorist outfits to operate with impunity online. While there has been no media reporting on the matter to prove this is or is not the case, in one instance in 2014, the Tehreek-e-Taliban Pakistan's newly launched website umarmedia.com was taken down within 24 hours, though it is unclear how or why this happened[41].

When the TTP site returned temporarily, according to a 2015 news report, "Senior officials admitted…that they had no effective legal mechanism to take down or block access to the website of the Tehreek-e-Taliban Pakistan (TTP), the banned outfit involved in most of the terrorist activities in the country." The officials cited a lack of legislation as the key problem as well as the fact that, "that many such outfits are operating websites under changed names, compounding the task of restricting public access.[42]"

Currently, the website appears to be blocked by the PTA.

[39] ***LHC orders media blackout of Altaf*** (2015, September, 8). Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1205555

[40] Walsh, D., Masood, S. (2014, June 6). ***Facebook under fire for temporarily blocking pages*** Retrieved on May 14, 2016, from The New York Times: http://www.nytimes.com/2014/06/07/world/asia/pakistan-facebook-blocked-users-from-political-pages-and-outspoken-rock-band-laal-against-taliban-.html

[41] Haider, J. (2014, April 7). ***TTP website taken down after 24 hours*** Retrieved on May 14, 2016, from Pakistan Today: http://www.pakistantoday.com.pk/2014/04/07/national/ttp-website-taken-down-after-24-hours/

[42] Khan, A. (2015, March 4). ***Unrestricted access: Cyber unit fails to disable or block TTP website*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/847366/unrestricted-access-cyber-units-fail-to-disable-or-block-ttp-website/

In the case of forcing publishers to self-censor through targeted social media campaigns, the most prominent targets have remained sites belonging to the English press. The social media campaigns, largely carried out on Twitter by the means of hashtags consisted of thousands of tweets containing hate speech, personal attacks and threats to the organisation and its members under the banner of being ‘anti-Pakistan’ e.g. the attack on the Dawn Media Group under the hashtag #DawnPawnofModi that came after the online release of an article on a lecture by a professor that suggested Pakistan had lost the 1965 war against India.

Similarly, the hashtag #bansexpresstribune against local daily The Express Tribune contained attacks for the publishing of articles questioning Pakistan’s relations with Israel, news reports on Baloch activists, pro-LGBT blogs, with the focus being on framing the paper as being ‘anti-Pakistan’ and ‘anti-Islam’.

# 1.2 CRIMINALISING ONLINE ACTIVITIES

Till 2014, the Pakistan Telecommunications Act 1996, The Pakistan Penal Code, the Anti-Terrorism Act 1997, the Defamation Ordinance 2002 and Defamation Amendment Act 2004 along with the Electronic Transactions Ordinance 2002 were the primary laws that criminalized legitimate freedom of expression online.

Since then, two major developments have taken place that will have a wide-ranging impact on criminalizing actions in cyberspace: the Protection of Pakistan Act, 2014 (PPA), and the Prevention of Electronic Crimes Bill (PECB).

## 1.2.1 PROTECTION OF PAKISTAN ACT, 2014

Passed into law in July, 2014, the PPA is “A Bill to provide for protection against waging of war or insurrection against Pakistan and the prevention of acts threatening the security of Pakistan.”[43] The law is framed to give the armed forces and law enforcement agencies sweeping powers to combat terrorism.

Within its Schedule of offences, “committed with the purpose of waging war or insurrection against Pakistan or threatening the security of Pakistan” is: (xiv) cyber-crimes, internet offences and other offences related to information technology which facilitates any offence under this Act.

The addition of section xiv, with no further definition of the terms used therein allow for all parts of the highly controversial act to apply to cyberspace. The Human Rights Commission of Pakistan described the Act as, “as a blatant attack on the fundamental rights of the people”. Similarly, Human Rights Watch condemned the Act, saying it threatens basic freedoms and rights in violation of Pakistan's international legal obligations.

With the passage of the Act, Pakistani internet users could face state action as suspected terrorists with the PPA’s many clauses coming into play, including preventive detentions that go into effect retrospectively; arrest and house searches without warrants including the use of force; the burden of proof lies on the suspect i.e. ‘guilty until proven innocent’; withholding of information on why a suspect is being held or where they are being held.

While such a case has not been recorded, the law remains a potent threat in terms of basic rights online, including speech that may be interpreted under the Act as “waging war” or “threatening the security” of the country.

[43] (Protection of Pakistan Act 2014, 2014)

## 1.2.2 PREVENTION OF ELECTRONIC CRIMES BILL

The PECB was passed in the National Assembly (NA) and will become law if the Senate moves the bill forward. The draft bill, which lay dormant for many years, was finally brought to the fore after the government announced the launch of the National Action Plan against terrorism. The draft bill has been seen as a 'key pillar' of NAP; an interior ministry implementation report stated that the bill was one of the 'cornerstones' of NAP in the crackdown on terrorists[44]. The draft bill passed by the NA proposes 14-year imprisonment or Rs50 million fine or both for those found guilty of cyber terrorism[45].

Controversial sections of the bill have included Section 4 and 7, which make whistleblowing a criminal act. The bill's language may: allow for the blocking of satirical content along with penalties; criminalize the use of VPNs that allow for private, encrypted browsing; criminalize communication that praises any person simply accused of a crime, not convicted.

The bill has been criticized by human rights activists, members of the IT industry and a handful of politicians for its harsh penalties, curtailing of human rights, giving law enforcement agencies sweeping powers and harming business[46].

Section 34 has remained the most highly criticized part of the PECB for its near-verbatim copying of a part of the Pakistan Constitution with no further definitions, thus giving agencies the power to interpret the Constitution to block any content online.

The section reads: "Power to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system: 1. The Authority is empowered to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system. The Authority or any officer authorized by it in this behalf may direct any service provider, to remove any intelligence or block access to such intelligence, if it considers it necessary 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 commission of or incitement to an offence under this Act."

[44] Abdullah, H., Yusuf, A., Zaidi, H. B. (2016, April 14). ***Electronic crimes bill: Big brother (and his brothers) are watching you*** Retrieved on May 30, 2016, from Dawn: http://www.dawn.com/news/1177610

[45] ***Prevention of electronic crimes act*** Retrieved on May 30, 2016, from Bolo Bhi: http://bolobhi.org/wp-content/uploads/2016/05/PECB-April-2016.pdf

[46] ***'Cybercrime draft violates constitution'*** (2015, April 16). Retrieved on May 30, 2016, from The News: http://www.thenews.com.pk/print/35224-cybercrime-draft-violates-constitution

## 1.3 IMPOSITION OF INTERMEDIARY LIABILITY

There is a pressing need to address the imposition of and protection from intermediary liability as the government, in the absence of legislation, has continued to block online content deemed ‘pornographic’, ‘blasphemous’ and ‘anti-state’.

Without intermediary liability legislation, the government has ultimate control in moderating ‘objectionable material’, as a result of which ISPs must follow PTA orders to block and filter access to specific websites or face license suspensions for not doing so.

Although the latest draft of the Prevention of Electronic Crime Bill 2014 provides for intermediary liability protection, the bill has not been passed into law yet (see Section 1.2.2.).

Despite this, a three-year ban on popular video sharing website YouTube was lifted earlier this year. The ban on YouTube   which remained in place from September 2013 to January 2016   was lifted when a localized version of the website was launched for Pakistan following an agreement between the government and Google (see Section 1.1.). The PECB bill, once passed by parliament, is to enable the government to pursue Google to give Pakistan rights to locally manage the content. The localized domain, which is to be moderated by the PTA, will be void of any “objectionable content”.

The issue of intermediary liability in this case was settled by handing over control to the state.

# 1.4 DISCONNECTING USERS FROM THE INTERNET

Most instances of disruption of internet services observed over the past year have been down to a suspension of cellphone services over the past year, with the occasional fault in undersea internet cables.

Pakistan is currently connected to the internet by means of four undersea fibre optic cables: the India-Middle East-Western Europe (I-ME-WE), SEA-ME-WE-3 and SEA-ME-WE-4 owned by PTCL and TWA-1 owned by TWA. A fifth submarine cable with a capacity of 24 terabits per second is expected to become operational by mid-2016. The cable will provide a backup in the event of a breakdown in one of the other submarine cables[47].

Pakistan's submarine cables developed major faults on at least two occasions in 2015 – SEA-ME-WE4 developed a fault in June[48], while I-ME-WE – which serves 80% of Pakistani users – broke down in December[49].

A more problematic trend is that of suspension of cellular services in various parts of the country for "security reasons"[50].

> "A problematic trend is that of suspension of cellular services for "security reasons"

Such suspensions were the norm in Karachi and Quetta by 2013, but the past year has seen more service suspensions occurring in Islamabad than in any other city, with cellphone services temporarily blocked in the capital for three consecutive Fridays in a bid to prevent Lal Masjid cleric Maulana Abdul Aziz from delivering sermons via cellphone during Friday prayers[51].

[47] Baloch, F. (2015, March 8). ***Broadband connectivity: New cable to provide faster access for consumers, businesses*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/849956/broadband-connectivity-new-cable-to-provide-faster-access-for-consumers-businesses/

[48] ***Damaged cables cause fluctuation in internet service.*** (2015, June 26). Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1190493

[49] ***Submarine cable fault affects PTCL broadband users.*** (2015, December 31). Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/1019239/browsing-issues-submarine-cable-fault-affects-ptcl-broadband-users/

[50] Haider, I. (2015, December 18). ***Cellphone services in Islamabad restored after temporary suspension*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1227173

[51] ***Mobile signals suspended for third Friday now.*** (2015, December 19). Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1227313

Cellphone services were suspended across the capital for at least three days due to a prolonged sit-in by protesters at D-Chowk following the chehlum of Mumtaz Qadri on March 27 [52].

A petitioner to the Islamabad High Court in April 2016 requested the court declare such suspensions of service illegal as it is apparently done without the statutory requirement of the president's 'Proclamation of Emergency'[53]. The court summoned the PTA and telecom operators, ordering them to issue a reply to the petition within a fortnight.

The suspension of services has been justified under the Pakistan Telecommunication (Reorganisation) Act under Section 54(3) pertaining to "national security". The law provides legal cover for disconnection of users from telecommunication services or the internet upon proclamation of emergency by the president.

In addition to suspension of service for "security reasons" in the wake of unusual incidents, suspensions have been commonplace during Muharram[54] and Eid[55].

Most recently, suspension of services in the capital on Pakistan Day, particularly in areas around the parade venue, were justified as "part of security measures"[56].

The suspension of services is viewed as extremely problematic within the context of connectivity of citizens - there are more 3G and 4G users than there are broadband users. And as more and more people rely on cellular connectivity for services and websites – especially life saving services such as access to ambulances/hospitals – the loss to consumers extends far beyond restrictions on communication.

[52] Ali, I., Haider, I., Bhatti, H., AFP. (2016, March 28). ***Nearly 2,000 pro-Qadri protesters continue sit-in outside Parliament.*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1248261

[53] ***Court summons PTA, cellular firms*** (2016, April 27). Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1254663

[54] ***Mobile service suspension: A cause of panic and massive socio-economic loss*** (2015, October 23). Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1214782

[55] Agencies. (2015, October 23). ***Mobile services to be suspended in some parts of the country: Malik.*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/743395

[56] Shahid, J. (2015, March 22). ***Islamabad citizens face cellphone, wireless services suspension*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1171188

# 1.5 CYBER ATTACKS

Pakistani internet users are one of the most at-risk populations in the world for malware attacks[57]. In addition to malware attacks, which can be used to steal personal information, Pakistanis face an unprecedented number of hacking attacks, especially from India, particularly during key events, such as Pak-India cricket matches or August 14th (Pakistan's Independence Day) and 15th (India's Independence Day)[58].

However, Pakistani hackers themselves have defaced over 2,000 Indian websites – or claim to have done so[59].

The Pak-India hacking war unofficially began back in 1998 when an Indian army website on Kashmir was defaced by Pakistani hackers. Since then, Pakistani and Indian hacking groups or 'hacktivists' have played a tit-for-tat game, with each hacking public and sometimes even private online infrastructure for what appear to be politically motivated reasons, though there is no proof that these groups are sanctioned or funded by their respective governments.

A US hacker, known for targeting Pakistani government websites, was released by the American government in 2014[60].

Government websites have begun to increasingly come under attack from hackers and other subversive elements attempting to steal sensitive data or intercepting privileged communications. Pakistani websites are attacked nearly daily with Distributed Denial of Service attacks and security breaches, mainly from India[61].

> "Pakistani websites are attacked nearly daily
> with DDOS attacks and security breaches"

[57] Chaudhry, H. (2016, May 6). ***Pakistan top target of malware attacks worldwide, says Microsoft*** Retrieved on May 14, 2016, from Dawn: https://www.dawn.com/news/1256601

[58] ***Pakistani, Indian website prone to cyber-attacks during key events: report*** (2016, February 12). Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/1045542/pakistani-indian-websites-prone-to-cyber-attacks-during-key-events-report/

[59] Baloch, F. (2014, February 2). ***Cyber warfare: Pakistani hackers claim defacing over 2,000 Indian websites*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/666537/cyber-warfare-pakistani-hackers-claim-defacing-over-2000-indian-websites/

[60] AFP. (2014, May 28). ***US hacker, who hacked Pakistani government websites, released.*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/714253/us-hacker-who-hacked-pakistani-government-websites-released/

[61] Cybercrimes: Pakistan lacks facilities to trace hackers (2015, February 1). Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers/

Most Pakistani ISPs, however, aren't capable of handling even small DDoS attacks, as a result of which, local businesses such as banking, call centers and BPO companies etc. suffer.

Even PTCL is not adequately equipped to counter coordinated attacks by cyber criminals and the impact of this could be disastrous as telecom companies control critical infrastructure. ISPs have been compromised on many occasions by hackers.

As recently as February 2015, the Federal Investigation Agency's cybercrime wing lacked the ability to cope with DDoS attacks, and was unable to trace attacks executed by hackers through proxies.

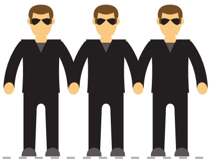
On a more micro level, the FIA has had to deal with crimes such as hacking of social media accounts, impersonation and harassment and blackmail – particularly of women. At least 18 such cases were reported last year[62].

In order to deal with cyber crime, the FIA, in the absence of a comprehensive cyber-crime law, has turned to outdated laws such as sections 36 and 37 of the Electronic Transaction Ordinance 2002 and Section 419 of the Pakistan Penal Code (see ILR 2013 for details). The scope of investigations is set to be broadened with the passage of the PECB (see Section 1.2.2.).

While cyber attacks can be dangerous on a personal level when sensitive information is involved, the government lacks infrastructure, training and laws in place to tackle cyber attacks seriously.

In addition, given the rapid spread of ICT, cellphones and 3G and 4G internet, putting insecure technology into the hands of people who are not aware how to protect themselves also puts others at risk. So far, the government has done little to increase awareness and education among users.

[62] Baloch, S. (2016, February 12). ***Suspect held for harassing woman through fake Facebook accounts.*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1238981



# 1.6 SURVEILLANCE

The Pakistani government has moved towards greater surveillance of users and networks through technological and legislative means since ILR 2013. There is increasing concern that local Law Enforcement Agencies (LEAs) and intelligence agencies have the ability to intrude into a range of devices to capture data, encrypted or otherwise.

The PTA and multiple security agencies, following guidelines set out by the government, courts and Ministry of IT, are able to conduct online surveillance and lawfully intercept and monitor data. LEAs and intelligence agencies either do so independently or turn to the FIA or PTA for assistance.

The Investigation for Fair Trial Act 2013 and the Pakistan Telecommunications (Re-organization) Act 1996 are two laws that permit authorities to collect privileged communication and grant broad surveillance powers. The PPA, and now the upcoming PECB draft bill also have provisions for greater surveillance in the interest of “national security” (see Section 1.2.).

In one high-profile case, the government had requested access to BlackBerry’s server e-mail and messaging content in order to conduct surveillance. In response, BlackBerry announced it would exit Pakistan rather than share users’ private data. In January this year however, BlackBerry announced it would stay in Pakistan. According to one news report, sources in the PTA said “the service provider has agreed to provide access to user’s data on demand only…we [PTA] would have to request the company, that we are investigating some suspect and need access to data, and company will provide us all the details and logs of that account”[63].

A recent Privacy International report uncovered that the government obtained ‘cyber security’ surveillance tools from multiple sources which enable high-level spying[64]. Those companies included big global players such as Nokia Siemens Networks, Alcatel, Ericsson, Huawei, SS8 and Utimaco. It was alleged that the military and agencies had received high levels of funding from foreign governments to develop infrastructure for surveillance in counter-insurgency efforts.

The PI report stated that the ISI was building a digital spy network to rival that of the United States. The ISI, it said, was planning to have access to Pakistan’s submarine internet cables. The investigation alleged that massive surveillance is already in place, and has been since

[63] (Khan, 2016)

[64] Rice, M. (2015, July 21). ***Tipping the scales: Security and surveillance in Pakistan*** Retrieved on May 30, 2016, from Privacy International: https://www.privacyinternational.org/node/624

2005. In a remark on the issue, the report stated that the public supported surveillance efforts given ongoing terrorism in Pakistan.

"ISI building a digital spy network to rival that of the United States: Privacy International report

The scenario outlined in the PI report was further corroborated by a 2015 leak of emails (hosted by WikiLeaks) of Hacking Team – an Italian company – that reveal Pakistani contractors had been trying to purchase invasive spy software for the government and local agencies for many years.[65]

Along with these efforts, the government has increased coordination with Facebook to access user accounts on the social network. This largely non-transparent act of surveillance has increased steadily since 2003 (see Section 1.0).

[65] ***The Hacking Team archives*** Retrieved on May 30, 2016, from Wikileaks: https://wikileaks.org/hackingteam/emails/

# 1.7 DATA PROTECTION

The schedule of offences in the PECB punishes “unauthorised” access to, copy or transmission of and interference with information systems or data (see Section 1.2.2.). However, it is important to note the distinction the draft bill makes between “lawful” and “unauthorised” access to data.

The latter refers to “access to such information system or data which is not available for access by general public, without authorization or in violation of the terms and conditions of the authorization”.

The above implies that while the “general public” is prevented from accessing sensitive data, the government or law enforcement agencies are permitted to do so, provided it is sanctioned by law. Lawful intercept of sensitive information by the abovementioned bodies is made possible through legislation and interception methods considered ‘lawful’.

However, Article 14(1) of the Pakistan Constitution ensures the right to privacy, and Article 8 states that laws that are inconsistent or in derogation of fundamental rights are void.

For the time being, the government appears to be surveilling and collecting data sanctioned through the 2002 Electronic Transaction Ordinance.

# 1.8 NET NEUTRALITY

There has been little formal debate over implementing legislation governing net neutrality in Pakistan.

Although Facebook's internet.org was introduced in Pakistan in March 2015, the service is only available over Telenor and provides access to select websites including AccuWeather, Facebook, BBC News, Bing, ESCPCrininfo, OLX and Wikipedia[66]. Local telcos have also begun the process of introducing 'zero rating' on some websites – including local sites – where customers' access to these platforms through their networks is offered free of charge.

The upcoming PECB does not address the issue of net neutrality as it focuses on "security" and "counter-terrorism" and does so by defining crimes and punishments for offences. The government's policy priority has almost solely been broadband proliferation as it contributes to the agenda of economic growth[67].

There is a need to make citizenry an active stakeholder in the establishment of a regulatory framework for net neutrality in Pakistan.

[66] ***Internet.org arrives in Pakistan*** (2015, May 29). Retrieved on May 14, 2016, from The News: http://www.thenews.com.pk/latest/4804-internet.org-arrives-in-pakistan

[67] APP. (2015, December 16). ***Pakistan calls for boosting int'l cooperation to end malicious use of ICTs in cyberspace*** Retrieved on May 30, 2016, from APP: http://www.app.com.pk/pakistan-calls-for-boosting-intl-cooperation-to-end-malicious-use-of-icts-in-cyberspace/

# 1.9 GOVERNMENT ENGAGEMENT ON AN INTERNATIONAL LEVEL

Although the Pakistani government has been active in the global conversation on the internet, especially within the context of counter-terrorism, there has been greater focus on state control – something that activists believe impinge upon personal freedoms, rather than protection of citizen's rights. Implementation of global standards and practices within Pakistan's internet landscape has been very limited, if at all.

Over the past year, Pakistani leaders have participated in seminars dealing with cyber security, although the outcome of such seminars appears to be minimal. Among the major global seminars, President Mamnoon Hussain was present at a Chinese government-organised conference where the Chinese President Xi Jinping urged greater cooperation in regulating internet use by means of a global governance system and encouraged the promotion of controls that activists believe impinge on freedom of expression, but which he said reflect "the wishes and interests of all countries"[68].

Mamnoon called for collective global efforts checking the abuse of cyberspace by terrorists and criminals. Mamnoon's views were echoed by IT Minister Anusha Rehman at the United Nations General Assembly, when she said that the "use of cyberspace by criminals and terrorists cannot be permitted".

The IT minister, however, went a step further, speaking of the need to agree on minimum standards of protection for "human dignity, particularly for women and children being the most vulnerable communities of cyberspace"[69].

While the PECB does address these issues human rights activists have pointed out that there is a lot of room for the law to be misinterpreted or misused[70].

Although there has been inter-governmental conversation regarding efforts towards counter terrorism, there has been little implementation of such measures or even the drafting of a framework for these measures.

[68] Agencies. (2015, December 17). ***China calls for cooperation on internet regulation*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1226876

[69] APP. (2015, December 17). ***Need stressed for cooperation to end malicious use of cyberspace*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1226903

[70] (Shahid, 2015)

## 2.1 RELEVANT MINISTRIES

### 2.1.1 PAKISTAN TELECOMMUNICATION AUTHORITY

Established in January 1997 under the Telecom Reorganization Act 1996[71], the PTA is the main regulatory and license issuing body overseeing the internet and telecom industry in Pakistan (See ILR 2013 for more details).

Since 2013, the PTA has taken on the role of the inter-ministerial committee for the evaluation of websites (IMCEW) which in previous years had determined which websites would be blocked in Pakistan.

The PTA took over this role after Prime Minister Nawaz Sharif disbanded the IMCEW after an Islamabad High Court (IHC) ruling that restrained the shadowy committee from blocking websites after it was challenged as acting illegally and contrary to the Telecom Act and Rules of Business 1973[72].

Some of the key events that the PTA was involved in over the last three years include:

- Ordering the banning of BlackBerry services[73]
- Recommending the unblocking of YouTube[74]
- Ordered the blocking of over 400,000 porn sites[75]
- Verified over 75 million SIMS & blocked 27.5 million in a national verification process[76]

[71] ***Pakistan Telecommunication (Re-organization) Act.*** (1996, October 17). The Gazette of Pakistan. Islamabad, Pakistan.

[72] Asad, M. (2015, January 11). ***Inter-ministerial body restrained from blocking websites*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1151146

[73] Gibbs, S., Agencies. (2015, July 27). ***Pakistan bans BlackBerry services in privacy crackdown*** Retrieved on May 14, 2016, from The Guardian: https://www.theguardian.com/technology/2015/jul/27/pakistan-bans-blackberry-messaging-internet-services-privacy-crackdown

[74] Musil, S. (2016, January 18). ***YouTube's years-long banishment in Pakistan ends – sort of*** Retrieved on May 14, 2016, from Cnet: http://www.cnet.com/news/youtubes-years-long-banishment-in-pakistan-ends-sort-of/

[75] Baloch, F. (2016, January 26). ***Pakistan to block over 400,000 porn websites*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/1034224/objectionable-content-isps-ordered-to-block-400000-pornographic-websites/

[76] APP. (2015, May 16). ***PTA blocks 27.m SIM cards as biometric verification process ends*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/887510/pta-blocks-27-5m-sim-cards-as-biometric-verification-process-ends/

- Coordinated blocking of Facebook pages with the company
- Sold 3G and 4G bands to local telcos for $1.1 billion[77]
- Temporarily suspended mobile phone services on multiple occasions
- Took part in the formulation and implementation of the Pakistan Telecommunication Policy 2015[78]

## 2.1.2 MINISTRY OF INFORMATION TECHNOLOGY

The federal MoIT is charged with initiating and launching IT and Telecommunications programs across Pakistan, along with establishing policies and legal framework and infrastructure for ICTs (See ILR 2013 for more details).

The major events related to cyberspace that the MoIT has been involved in since 2013 include:

- The years-long ban on YouTube and the site's eventual unblocking
- The preparation and submission of the PECB draft[79].
- The sale of 3G/4G bands in Pakistan

The ministry, and specifically its minister Anusha Rehman, has been the target of heavy criticism by the public, media and digital rights groups since ILR 2013 for its role in online censorship and the justification of such bans, as well as its drafting and advocacy for the highly controversial PECB (see Section 1.2.2.).

## 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, smuggling as well as copyright infringement and other specific crimes. The FIA's National Response Centre for Cyber Crimes (NR3C) wing is responsible for taking action against crimes committed on the internet, and accordingly, the agency is greatly involved in online surveillance (See ILR 2013 for more details).

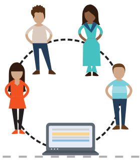
[77] Bhatti, S. I., Reuters. (2014, April 24). ***$1.1 billion raised from 3G, 4G auction*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1101760

[78] Aftab, M. (2016, February 1). ***Pakistan's new telecom policy to boost growth*** Retrieved on May 14, 2016, from Khaleej Times: http://www.khaleejtimes.com/international/pakistan/pakistans-new-telecom-policy-to-boost-growth

[79] ***Draft Prevention of Electronic Crimes Bill 2015.*** (2015, September 17). Retrieved on May 14, 2016, from the Ministry of IT: http://www.moitt.gov.pk/gop/index.php?q=aHR0cDovLzE5Mi4xNjguNzAuMTM2L21vaXQvZnJtRGV0YWlscy5hc3B4P29wdD1taXNjbGlua3MmaWQ9NTI%3D

In the last two years the major events the NR3C has been a part of include:

- A series of raids and arrests of individuals and gangs involved in the harassment of citizens, particularly female, in the online space.
- Reduction in grey traffic through action against those running illegal gateway exchanges.
- Investigating and arresting criminals involved in online fraud cases and scams.
- The arrest of numerous hackers.
- Working with Facebook and other social media sites in online investigations.



# 2.2 IMPORTANT STAKEHOLDERS

## 2.2.1 POLITICIANS

The role of politicians in shaping the future of the internet in Pakistan has largely consisted of reactive statements to events or non-participation despite their key role in shaping the future of the internet as lawmakers (See ILR 2013 for more details).

Only a handful of politicians have taken an interest/been involved in developments that impact cyberspace since ILR 2013, continuing a trend that has been seen for many years. The most high-profile – and most highly criticized for backing of regressive acts and policies – politician has been Minister of IT, the PML-N's Anusha Rehman. Under her steering, the PML-N led government's role has been that of justifying censorship as in the case of the YouTube ban, facilitating the passing of the highly controversial PPA, and most recently, a push for passing of the PECB.

In the case of passing the PPA (see Section x) into law, after a brief outburst on its introduction in Parliament[80], politicians did not engage in rigorous debate (with no reported discussion related to its extension to cyberspace)[81], and in fact, showed very little resistance to the bill as it was originally written. Minister for Science and Technology Zahid Hamid presented the bill in the National Assembly and Senate in its passing with consensus from all political parties with a few amendments[82].

In the case of the PECB (see Section x), greater resistance was seen on the part of individual politicians but the controversial bill was passed by the National Assembly's Standing Committee on Information Technology without consideration of the many objections raised against it. As one report noted, at this critical stage, "A majority of members failed to turn up at the meeting, paving way for Pakistan Muslim League-Nawaz (PML-N) legislators to surpass those critical of the legislation, including the media, internet service providers, NGOs and members of civil society."

Objections were however raised by the MQM's Syed Ali Raza Abidi, PPP MNAs Shazia Marri (who was most vocal in opposing the bill) and Nauman Islam Sheikh, PTI MNA Amjad Ali

[80] Khan, A. (2014, April3). ***Protection of Pakistan Ordinance: Govt moves controversial bill in National Assembly*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/690727/protection-of-pakistan-ordinance-govt-moves-controversial-bill-in-national-assembly/

[81] Haider, I. (2014, July 2). ***Protection of Pakistan Bill 2014 approved in NA*** Retrieved on May 14, 2016, from Dawn: http://www.dawn.com/news/1116529

[82] Firdous, I. (2014, June 30) ***Senate passes amended Protection of Pakistan Bill 2014*** Retrieved on May 14, 2016, from The Express Tribune: http://tribune.com.pk/story/729238/senate-passes-the-protection-of-pakistan-bill-2014/

Khan and PML-N members Awais Ahmad Khan Leghari and Khusro Bakhtyar. The bill was passed in the National Assembly, where the PML-N government held the majority, with only 30 of 342 members present[83].

Some senators raised objections to the bill's passing, with Standing Committee on Information Technology and Telecommunication Chairman Senator Shahi Syed going as far as saying that he will not let the bill pass in Senate[84].

The effort to introduce cyber security to Pakistan by Chairman of Senate Defence Committee Senator Mushahid Hussain (outlined in ILR 2013) also remained a hypothetical over the last two years. In a talk in 2015, Senator Mushahid Husaain reiterated the need for a "Computer Emergency Response Team (CERT), a Joint Inter-Services Cyber Defence Command, and Cyber 'rules of the game' within the SAARC framework between Pakistan and India to ensure that neither side engages in cyber warfare"[85]. None of these have since been realized.

## 2.2.2 ISPs

Pakistan's ISPs are directly tied into the growth and challenges presented by the internet. There are at least 50 operational ISPs providing internet services, of which 10 provide high-speed services[86]. The ISPs and PTCL in particular drive investment and overall growth of the internet. However, the role of cellular service providers operating in Pakistan – Mobilink, Telenor, Warid, Ufone and Zong – has now become paramount as well, given their operation of 3G, 4G and EDGE networks that provides their customers internet connectivity on their phones and through various other products/services.

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 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[87]. Aside from TWA, the company still controls most of the bandwidth in Pakistan.

PTCL 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 the majority of bandwidth in the country. Other big players include Wateen, Qubee, Comsats, LINKdotNET, World Call

[83] ***ISPAK*** (2012, April 26). Retrieved May 14, 2016, from Internet Service Providers Association of Pakistan: http://www.ispak.pk/

[84] ***Pakistan profile 2012*** Retrieved on May 14, 2016, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan

[85] ***Top sites in Pakistan*** Retrieved on May 14, 2016, from Alexa: http://www.alexa.com/topsites/countries/PK

[86] Asad, M. (2014, December 2). ***ISI and the military lodge complaint against fake Facebook accounts*** Retrieved on July 3, 2016, from Dawn: http://www.dawn.com/news/1148229

[87] ***Pakistan.*** (2012, August 6). Retrieved on September 15, 2013, from OpenNet Initiative: https://opennet.net/research/profiles/pakistan

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.

## 2.2.3 MEDIA

Private media groups are a powerful stakeholder in their ability to challenge the state and raise issues related to the internet in multiple mediums, including online.

Over 100 TV channels are operated in Pakistan by private media groups, broadly divided into entertainment/lifestyle, news, religion, sports and regional language channels. Additionally, the state-operated PTV network is available, as is the newer, more-expensive digital offerings that include many international TV channels. While the print industry has shrunk since the broadcast media boom of the Musharraf-era, there are still hundreds of newspapers and magazines (majority in Urdu or regional languages) that hold considerable influence over large audiences. Additionally, FM stations operated in urban areas of Pakistan also have wide reach.

Cross-media ownership dominates the industry, with some media groups operating across TV, print, radio and online. Many others operate with TV, print and digital brands under one banner. As a consequence, agendas set by the media groups attain wide reach through a consistent messages across the many mediums they operate.

These media groups form a considerable chunk of the top 100 visited sites in Pakistan[88], along with operating some of the large local social media networks for their various brands. Policies with regards to cyberspace e.g. online censorship have a direct impact on these groups in the form of banning of sites or blocking of social media accounts. Online surveillance is also a threat, especially for journalists working in newspapers, TV news channels and online.

Despite this, with the exception of English print media, coverage of internet-related issues such as censorship, blocking or filtering, access and the digital divide and legislative developments like PECB has been largely reactive and fleeting. Even more problematic is the media's often ill-informed tackling of the issues due to a lack of training in a specialized field, and due to the influence of the state on media groups, and particularly owners[89]. Most worryingly, the Urdu press and some TV channels being actively in favor of state policy and actions. In general however, the media only tends to respond to high profile cases of

[88] ***Top sites in Pakistan.*** (2013). Retrieved on September 20, 2013, from Alexa: http://www.alexa.com/topsites/countries/PK

[89] (Yusuf, 2013)

censorship or arrests that involve online blasphemy (e.g. Facebook ban, YouTube ban) with coverage focused less on the issue and more on street protests and religious debate. On occasion censorship related to pornography is covered, but only as cursory news reports following PTA or Supreme Court orders. In the case of the passing of the PECB, much of the debate in mainstream media has focused on reporting of events and the politics behind the bill, with its content being a secondary focus.

## 2.2.4 MILITARY

The military has consolidated power since ILR 2013 following the Army Public School attack that led to the National Action Plan (NAP) against terror.
The role of the military has been paramount in the censorship of cyberspace since the early blocking of Baloch separatists websites. In addition to blocking content deemed 'anti-state', content that is seen as directly damaging to the image of the military has been censored. Pakistan's top brass have been victims of online impersonation, leading to a crackdown on fake social media accounts in 2014. A request was lodged by the PTA with Facebook to shut down fake accounts of army and intelligence personnel. Facebook complied, but the profiles cropped up again later[90].

Aside from blocking online spaces, the military and spy agencies continue to build out their online surveillance systems aggressively in the context of the continuing war against terrorists (see Section 1.2.).

In all, the military's involvement in the internet has been largely intrusive and regressive to date. As arguably the most powerful player in the future of cyberspace after the National Action Plan has come into play, the military's decisions will likely come to define the internet in Pakistan, with all stakeholders following suit.

## 2.2.5 TERRORIST / EXTREMIST OUTFITS

A number of terrorists, extremist outfits and militants, despite being banned by the government of Pakistan, continue to operate with near-impunity in the online space due to lack of effective regulation.

According to the government, banned organizations have at least 3,000 websites promoting their ideology in Pakistan[91]. In addition to websites, groups such as the Tehreek-i-Taliban

[90] (Asad, 2014)

[91] ***Terrorists operating 3,000 websites in the country, NA told*** (2015, Aug 14). Retrieved on May 30, 2016, from Pakistan Today: http://www.pakistantoday.com.pk/2015/08/14/national/terrorists-operating-3000-websites-in-country-na-told/

Pakistan, Daesh, Sipah-i-Sahaba, Lashkar-i-Jhangvi and Lashkar-i-Taiba continue to use social media and telecommunications to spread hate, recruit members, issue threats, coordinate and claim responsibility for attacks.

In 2014, the TTP launched a website that was later banned by the Pakistani government, the terrorist group continues to administer a Facebook page and utilises Gmail for communication purposes. The Hizbut Tahrir has multiple websites, at least one of which has not been banned.

Although law enforcement agencies have begun to take notice of and occasionally crackdown on hate speech in the online space[92], there are no reports of a sustained effort on this front. Even the few cases where action has been taken remain suspect for the motivation prompting action (e.g. in blasphemy cases), given that larger banned outfits remain untouched.

The government has however moved to introduce harsh legislation (see Section X) to clamp down on militant activity online, with the introduction of the term cyber terrorist in the PECB for those committing a number of offenses such as spreading extremist ideologies, sectarian hatred, calls to violence, overthrow of the government etc. While ill-defined, the PPA also allows for action against terrorists/extremist outfits under its many clauses. But legislation is only a small part of a concrete solution, in which time, banned groups continue operations online.

## 2.2.6 NGOs AND CIVIL SOCIETY

A handful of NGOs and civil society embers remain active on issues pertaining to the internet and human rights and freedoms online e.g. with members of both groups taken on board by the government when drafting the PECB[93].

However, the government's consultation of these stakeholders has been termed inadequate, and lawmakers question who the real stakeholders are when it comes to the cyber crime bill[94]. These entities have urged the government to scrap the bill for violating human rights[95] and providing vague definitions[96].

[92] AFP. (2016, March 4). ***Pakistani man sentenced to 13 years in prison for 'posting religiously offensive material on Facebook'*** Retrieved on May 30, 2016, from The Nation: http://nation.com.pk/national/04-Mar-2016/pakistani-man-sentenced-to-13-years-in-prison-for-posting-religiously-offensive-material-on

[93] ***Pakistan country report 2015*** Retrieved on May 30, 2016, from Freedom On The Net: https://freedomhouse.org/report/freedom-net/2015/pakistan

[94] Shahid, J. (2015, August 7). ***IT ministry in the dark about status of cyber crime bill*** Retrieved on May 30, 2016, from Dawn: http://www.dawn.com/news/1198945

[95] ***Civil society urges govt to scrap cybercrime bill for violating human rights*** (2015, December 1). Retrieved on May 30, 2016, from Dawn: http://www.dawn.com/news/1223517

[96] ***Pakistan country report 2015*** Retrieved on May 30, 2016, from Freedom On The Net: https://freedomhouse.org/report/freedom-net/2015/pakistan

The draft bill went back to the drawing board after heavy criticism[97], but the ‘final’ draft presented later in 2015 reflected little of the feedback offered by civil society stakeholders and was not made available to all during the consultation before being passed on to the National Assembly[98].

Civil society protested strongly over the PPA, saying that the language which criminalises unspecified cyber crimes as acts of terror is vague and open to abuse[99].

Civil society groups and NGOs have also spoken up against the indiscriminate blocking and filtering of websites, as well as arbitrary blocks on VPNs, with certain groups taking the matter to court most notably, in the case of YouTube and the film ‘The Innocence of Muslims’[100].

Bytes For All campaigned against excessive surveillance and use of malware to intercept communications and private information by petitioning the Lahore High Court against the use of Fin Fisher by parties inside Pakistan in 2013. Although the court ordered the PTA to submit a report on the matter, further hearings on the issue have been unsuccessful[101].

Certain civil society organisations and NGOs play a role in educating and training at-risk groups such as women, minorities and journalists in internet literacy. The Digital Rights Foundation holds such trainings on a regular basis.

In general, the role of larger civil society has been limited, most often in the form of online public protests in reaction to events such as the blocking of rock band Laal’s Facebook page (see Section 1.1.3.). While such occasional protests have been successful, the only sustained efforts related to the internet have come from a handful of NGOs working on digital rights and internet-related issues.

[97] ***Open platform: Cybercrime bill flayed by social activists, NGOs*** (2015, August 20). Retrieved on May 30, 2016, from The Express Tribune: http://tribune.com.pk/story/941198/open-platform-cybercrime-bill-flayed-by-social-activists-ngos/

[98] Shahid, J. (2015, September 18). ***Draft cybercrime bill bulldozed through NA body*** Retrieved on May 30, 2016, from Dawn: http://www.dawn.com/news/1207737

[99] Pakistan country report 2015 Retrieved on May 30, 2016, from Freedom On The Net: https://freedomhouse.org/report/freedom-net/2015/pakistan

[100] Pakistan country report 2015 Retrieved on May 30, 2016, from Freedom On The Net: https://freedomhouse.org/report/freedom-net/2015/pakistan

[101] State of surveillance in Pakistan Retrieved on May 30, 2016, from Privacy International: https://www.privacyinternational.org/node/734

# ABOUT BYTES FOR ALL, PAKISTAN

Bytes for All (B4A), Pakistan is a human rights organization and a research think tank with a focus on Information and Communication Technologies (ICTs). It experiments with and organizes debate on the relevance of ICTs for sustainable development and strengthening human rights movements in the country. Its strategic plan delivers in following key result areas (KRA), which include:

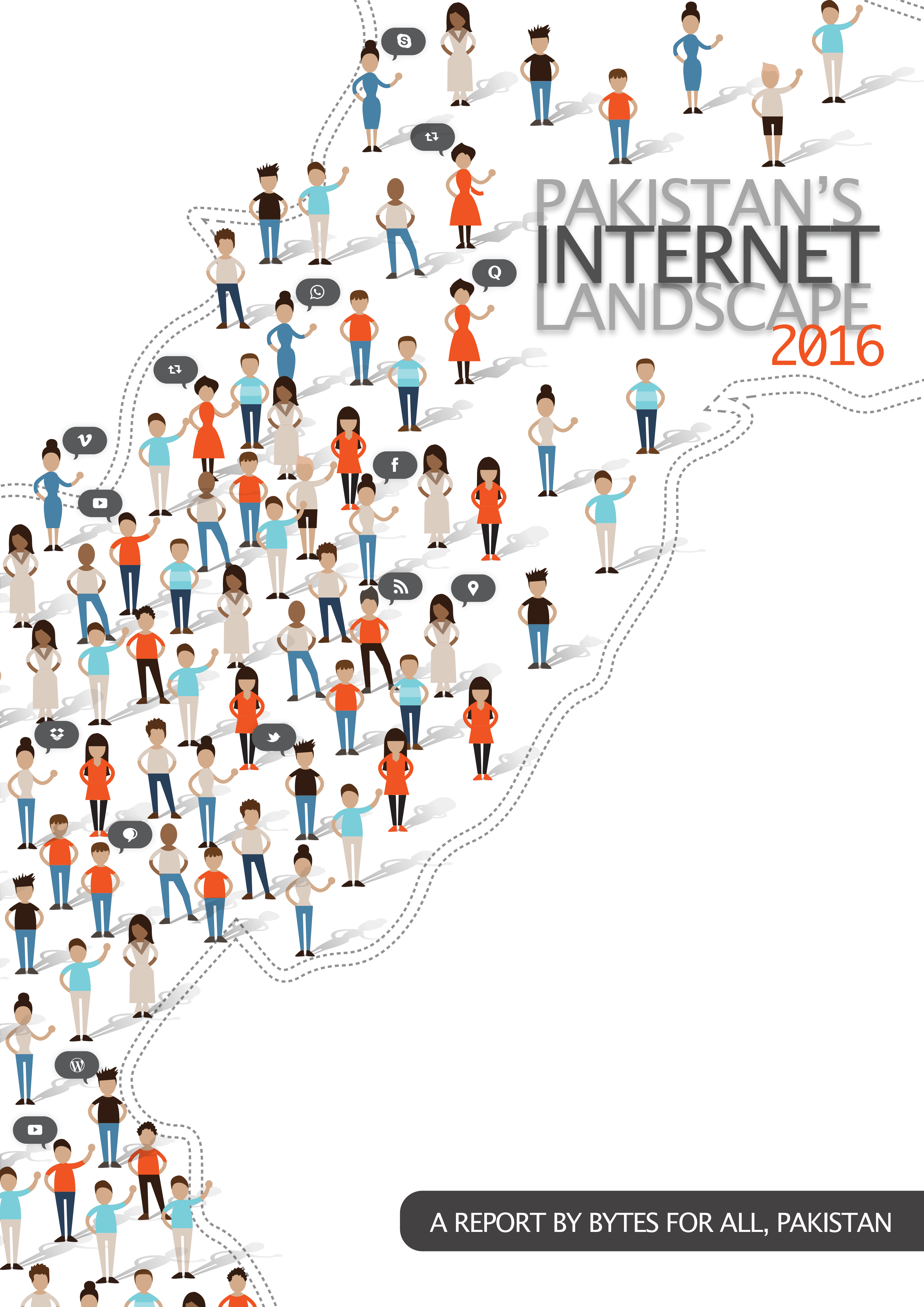
1. Securing digital rights and freedom of expression for civil liberties;
2. Strengthening digital security of human rights defenders & media professionals;
3. Ending technology-driven gender-based violence;
4. Network building at national, regional and global level; and
5. Community development and communications for environmental sustainability

To deliver above-mentioned KRAs, B4A conducts research for evidence-based policy advocacy and capacity building of human rights defenders on their digital security, online safety & privacy.

Globally acclaimed Take Back The Tech Campaign is the flagship of Bytes for All, which focuses on strategic use of ICTs by women and girls to fight violence against women in Pakistan.

**Bytes for All, Pakistan**
info@bytesforall.pk | @bytesforall
www.bytesforall.pk

www.bytesforall.pk



# PAKISTAN'S INTERNET LANDSCAPE 2016

A REPORT BY BYTES FOR ALL, PAKISTAN