Freedom House

Pakistan

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	20	18
Limits on Content (0-35)	20	20
Violations of User Rights (0-40)	29	31
TOTAL* (0-100)	**69**	**69**

* 0=most free, 100=least free

Population:	**188.9 million**
Internet Penetration 2015 (ITU):	**18 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The National Assembly approved the Prevention of Electronic Crimes Act, including clauses which would enable censorship, surveillance, and rights violations (see **Legal Environment**).
- In January 2016, YouTube was unblocked for the first time since 2012, redirecting users to a local version, YouTube PK (see **Blocking and Filtering**).
- Antiterrorism courts sentenced two individuals to 13 years in prison each in separate cases involving charges of promoting religious or sectarian hatred on Facebook (see **Prosecutions and Detentions for Online Activities**).
- Investigators charged a man in Peshawar with violating "privacy of information" and "damage to information systems" based on Twitter posts he wrote about a judge's relatives in September 2015 (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom remained repressive in Pakistan in 2015-16, where the unblocking of YouTube was overshadowed by harsh punishments for online speech.

The Prevention of Electronic Crimes Bill, draft cybercrime legislation with scope to suppress free expression, came under intense criticism in 2015, in Pakistan and from international rights organizations and the United Nations Special Rapporteur on freedom of opinion and expression. On April 13, 2016, however, an amended bill that retained many problematic clauses was approved by the National Assembly. The Senate approved the bill outside the coverage period of this report, and it was adopted in August.[1]

New legal measures are particularly concerning in light of harsh punishments for online expression handed down in 2015 and 2016. Antiterrorism courts sentenced two men in separate cases to 13 years imprisonment for allegedly distributing "hateful" or "sectarian" material about religion on Facebook. Separately, individuals communicating online were charged under the 2002 Electronic Transactions Ordinance, an early ecommerce law, including a member of the Pakistan Tehreek-i-Insaf party who wrote about a judge on Twitter.

In a positive development, a local version of the popular video-sharing platform YouTube was made available for the first time since 2012, when the entire platform was blocked for hosting the anti-Islamic video, "The Innocence of Muslims." Users feared YouTube PK would be subject to stricter censorship than its international counterpart. Separately, Blackberry negotiated to continue offering encrypted messaging services in Pakistan after the government warned them they would need to shut down operations if they did not grant officials access to the content being exchanged through their servers.

Obstacles to Access

Internet penetration is limited in Pakistan by a lack of resources and infrastructure, but mobile internet access is increasing following the recent launch of faster 3G and 4G service. However, Pakistani authorities frequently disable mobile internet access during times of perceived political or religious sensitivity.

Availability and Ease of Access

The International Telecommunication Union reported internet penetration at 18 percent in 2015, based on figures from the Pakistan Bureau of Statistics.[2] Pakistan's telecommunications regulator reported mobile penetration at 73 percent.[3] Internet penetration is expected to increase with the recent launch of 3G and 4G technology (see ICT Market). While the cost of internet use has fallen considerably in the last few years,[4] with prices around US$12 a month for a broadband package in 2015, access remains out of reach for the majority of the population.

1 Reuters, "Pakistan passes controversial cyber-crime law," August 12, 2016, http://www.reuters.com/article/us-pakistan-internet-idUSKCN10N0ST.

2 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

3 "Cellular subscribers reach 132.33m with 73.5pc record penetration," *Pakistan Today*, February 10, 2014,http://bit.ly/1Nvtn8n.

4 "Average monthly Internet cost in Pakistan low," *Daily Times*, October 3, 2015, http://bit.ly/1N4iCa3.

Broadband subscriptions, based on DSL—which uses existing telephone networks—or wireless Wi-Max technology, are concentrated in urban areas. Most remote areas lack broadband, and a large number of users depend on slow dial-up connections or EDGE, an early mobile internet technology. In such areas, meaningful online activity like multimedia training can be challenging, though faster 3G and 4G networks are making inroads, albeit at a slow pace. Several parts of western areas of Pakistan lack internet access, partly because of underdevelopment and partly because of ongoing conflict. According to one study, more than 75 percent of tribal areas and 60 percent of Balochistan province lacked fiber optic connections in 2013. [5]

Low literacy, difficult economic conditions, and cultural resistance have limited the proliferation of ICTs in Pakistan.[6] Though internet access is gradually increasing among girls and women, online harassment unfortunately discourages greater utilization of ICTs by women, especially those under 30. Reports of criminal harassment on social media are frequent (see Intimidation and Violence).

Increasing security measures mean that users must register their fingerprints along with other identifying information when applying for broadband internet packages and mobile service. This has worrying implications for human rights activists and others who rely on anonymous internet access, and may discourage some from seeking home service. Unregistered phones were subject to disconnection in 2015 (see Surveillance, Privacy, and Anonymity).

Restrictions on Connectivity

The predominantly state-owned Pakistan Telecommunication Company Limited (PTCL) controls the country's largest internet exchange point, Pakistan Internet Exchange (PIE), which has three main nodes—in Karachi, Islamabad, and Lahore—and 42 smaller nodes nationwide. PIE operated the nation's sole internet backbone until 2009, when additional bandwidth was offered by TransWorld Associates on its private fiber-optic cable, TW1.[7]

PTCL also controls access to the three international undersea fiber-optic cables: SEA-ME-WE 3 and SEA-ME-WE 4 connect Southeast Asia, the Middle East, and Western Europe; and I-ME-WE links India, the Middle East and Western Europe.[8] The company signed an agreement to build the fourth cable, considered to be one of the world's largest, in 2014. The AAE-1 cable, projected to be completed by the end of 2016, will connect countries in Asia, Africa, and Europe.[9]

Damage to these cables did not cause widespread access disruptions during the coverage period, as it has done in the past.[10] In early 2015, villages in the northern Drosh Valley faced internet and telephone disconnection because of damage to the open main cable.[11] As in previous years, however, Pakistan faced electricity shortages in 2015 and 2016, especially when demand peaked during the

5 Zakir Syed, "Overcoming the Digital Divide: The Need for Modern Telecommunication Infrastructure in the Federally Administered Tribal Areas (FATA) of Pakistan," *Tigah Journal* (2013) http://bit.ly/1LulYiV.

6 Arzak Khan, "Gender Dimensions of the Information Communication Technologies for Development," (Karlstad: University of Karlstad Press, 2011) doi: http://dx.doi.org/10.2139/ssrn.1829989.

7 OpenNet Initiative, "Country Profile—Pakistan," August 6, 2012, http://bit.ly/1LDXNEX.

8 "PTCL Expects 20pc Growth with Launch of IMEWE Cable: Official," *The News*, December 22, 2010, http://bit.ly/1huHRXs.

9 "PTCL to build largest int'l submarine cable consortium system," *Daily Times*, January 30, 2014, http://bit.ly/1L4dxO6; "AAE-1 subsea cable lands at Crete", *Capacity Media, April 19, 2016, http://bit.ly/1qXbCFs*

10 Farooq Baloch, "Undersea Cable Cut Affects 50% of Pakistan's Internet Traffic," *Express Tribune*, March 27, 2013, http://bit.ly/1FWOnSV.

11 Gul Hamaad Farooqi, "Chitral villages lack phone, internet facilities," *The Nation*, February 10, 2015, http://bit.ly/1GAOiPi.

summer months.

Security considerations continued to intrude on telecommunication services. In 2015 and 2016, as in previous years, the government suspended cellular services on some religious and national holidays on grounds that terrorists could use the networks to coordinate violent acts. In October 2015, for example, the Interior Minister directed cellular service operators to block service in parts of the country during the religious holiday Eid-ul-Fitr.[12] A 2015 report highlighted that shutting down cellular services places citizens at risk, rather than protect them. Both the state and telecommunications providers have lost millions in revenue during past shutdowns, according to the report.[13]

Orders to suspend service cite Section 54 of the 1996 Pakistan Telecommunications Act, though this should only apply during a state of emergency. The use of the law to support service suspension orders has been challenged in the Sindh High Court by Telenor Pakistan and a doctor who reported being unable to communicate with patients during a shutdown, among others. In 2016, the court had yet to issue a decision in those cases, which date from 2012.[14]

ICT Market

In the latest available data, the Internet Service Providers Association of Pakistan reported 50 ISPs operational in Pakistan as of October 2014; 10 of those provide DSL services.[15] The government regulator, the Pakistan Telecommunication Authority (PTA), exerts significant control over internet and mobile providers through a bureaucratic process that includes hefty licensing fees.[16]

The predominantly-state-owned Pakistan Telecommunication Company Limited (PTCL) controls 60 percent of the broadband market. [17] In 2012, an antimonopoly inquiry said the prices it charged other companies to use its infrastructure had forced private DSL operators to leave the market, which PTCL denied.[18]

After several years delay, Pakistan finally introduced internet-capable 3G mobile network and 4G spectrum, in 2014. The 3G spectrum auction was won by four foreign-owned companies, Mobilink, Zong, Telenor, and Ufone; Zong also won 4G spectrum. Pakistan secured US$903 million and US$210 million from the 3G and 4G spectrum auctions, respectively. These networks will provide faster internet services to consumers in Pakistan.[19] Although so far limited to urban centers, mobile companies report that they are rapidly expanding the networks.[20]

Internet cafes do not require a license to operate, and opening one is relatively easy.[21] Child rights

12 "Mobile phones services to be suspended in parts of country: Malik" *Dawn*, October 23, 2015, http://bit.ly/28Ifl6j

13 "Mobile service suspension: A cause of panic and massive socio-economic loss". *Dawn*, October 23, 2015 http://www.dawn.com/news/1214782; Institute for Human Rights and Business, "Security v Access: The Impact of Mobile Network Shutdowns, Case Study Telenor Pakistan," September 2015, http://www.global.asc.upenn.edu/publications/security-v-access-the-impact-of-mobile-network-shutdowns-case-study-telenor-pakistan/.

14 "Security v Access: The Impact of Mobile Network Shutdowns, Case Study Telenor Pakistan."

15 Internet Service Providers Association of Pakistan, http://www.ispak.pk/.

16 Pakistan Telecommunication Authority, "Functions and Responsibilities," December 24, 2004, http://bit.ly/1OpRm9c.

17 Adam Senft, et al., *O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Net sweeper's Role in Pakistan's Censorship Regime,* Citizen Lab, June 20, 2013, https://citizenlab.org/2013/06/o-pakistan/.

18 Iftikhar A. Khan, "PTCL forces half of DSL operators to quit," *Dawn*, June 20, 2012, http://bit.ly/1VJTOLT.

19 Sohail Iqbal Bhatti, "$1.1 billion raised from 3G, 4G auction," *Dawn*, April 24, 2014, http://www.dawn.com/news/1101760.

20 "In demand: 3G user base expanding, market surges forward," *The Express Tribune*, September 16, 2014, http://bit.ly/1L4ebv8.

21 Sehrish Wasif, "Dens of sleaze," *Express Tribune*, July 22, 2010, http://tribune.com.pk/story/29455/dens-of-sleaze/.

groups have argued that cafes should be regulated to prevent inappropriate access to pornography and gambling sites.[22]

Regulatory Bodies

The PTA is the regulatory body for the internet and mobile industry, and international free expression groups and experts have serious reservations about its openness and independence.[23] The prime minister appoints the chair and members of the three-person authority, which reports to the Ministry of Information Technology and Telecommunication.[24] The repeated failure to make new appointments since 2013 have further undermined the PTA's reputation. In March 2015, the PTA formally took responsibility for internet content management (see Blocking and Filtering).

In December 2015, Pakistan's Economic Coordination Council approved the Government of Pakistan's Telecommunications Policy 2015. [25] The Policy outlines and addresses issues faced by some network operators and also reinforces the PTA's authority to "monitor and manage content" online.[26] However, the Telecoms Policy does not address concerns from the telecoms industry in Pakistan in regards to the suspension of cellular services during religious or national holidays for security reasons. The Policy has been criticized for not addressing obstacles to greater internet penetration in a manner that offers fair pricing and choices for the consumer.[28]

Limits on Content

The Prevention of Electronic Crimes Act authorizes the PTA to undertake content management. In January 2016, YouTube was unblocked, but users in Pakistan can only visit a version subject to local laws restricting content. Other platforms, media, and communication tools are popular and contribute to a vibrant online space.

Blocking and Filtering

In April 2016, the National Assembly approved the Prevention of Electronic Crimes Act (see Legal Environment). It was later approved by the Senate, and passed in August. Section 37 authorizes the PTA to "issue directions for removal or blocking of access of any information through any information system" it considers necessary for "the glory of Islam or the integrity, security or defense of Pakistan… public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act."[27]

The task of ordering blocks was formerly undertaken by the Inter-Ministerial Committee for the Evaluation of Web Sites (IMCEW), comprised of representatives from PTA and the government, along

22 Qaiser Butt, "Dirty business in sequestered cubicles," The Express Tribune, February 16, 2015, http://bit.ly/1L4ekif.

23 Article 19, "Pakistan: Telecommunications (Re-organization) Act," legal analysis, February 2, 2012, http://bit.ly/1Pl5OOR.

24 Pakistan Telecommunication Authority, "Pakistan Telecommunication (Re-organization) Act 1996," *The Gazette of Pakistan,* October 17, 1996, http://bit.ly/16sASJI.

25 "ECC approves Telecom Policy 2015", *Pakistan Today*, December 12, 2015 http://bit.ly/1QTPqBo.

26 "An Overview of Telecom Policy 2015", Propakistani, December 12, 2015, http://propakistani.pk/2015/12/12/an-overview-of-telecom-policy-2015/

27 "Pak Telecom policy 2015 – another step forward for censorship" Digital Rights Foundation, February 10, 2016 http://bit.ly/1QTQAg9; http://digitalrightsfoundation.pk/wp-content/uploads/2016/08/PECB2016.pdf

with "men from the Ministry of Religious Affairs, the Inter-Services Intelligence, and Military Intelligence."[28] In March 2015, at the request of the Ministry of Information,[29] Prime Minister Sharif disbanded the Inter-Ministerial Committee and authorized the PTA to undertake content management.[30] The Prevention of Electronic Crimes Act provides the legal authority for this activity.

The Telecommunications Policy approved in December 2015 (see Regulatory Bodies) utilized similar language. Section 9.8.3 states that the PTA will be enabled to "monitor and manage content including any blasphemous and pornographic material in conflict with the principles of Islamic way of life as reflected in the Objectives Resolution and Article 31 of the Constitution" as well as material that is considered to be "detrimental to national security, or any other category stipulated in any other law."[28]

Overly broad provisions in the 1996 Pakistan Telecommunications Act already support censorship for the protection of national security or religious reasons.[31] Section 99 of the penal code allows the government to restrict information that might be prejudicial to the national interest, to justify filtering antimilitary, blasphemous, or antistate content.[32] Critics believe these issues can serve as cover for politically motivated censorship of dissenting voices. Information perceived as damaging to the image of the military or top politicians, for example, is also targeted.

Historically, blocking orders have directed ISPs and backbone providers to implement manual blocks on individual URLs or IP addresses, their compliance ensured by licensing conditions. [33] Since 2012, successive administrations have sought to introduce technical filtering.[34] The National ICT Research and Development Fund initially requested that companies develop nationwide blocking technology to "handle a block list of up to 50 million URLs," [35] though the status of that project was left in doubt after widespread civil society protests.[36] News reports in 2013 and 2014 said PTA and government officials were still pursuing filtering solutions.[37] In 2013, the University of Toronto-based research group Citizen Lab reported that technology developed by the Canadian company Netsweeper was already filtering political and social content at the national level on the PTCL network.[38] "In addition to using Netsweeper technology to block websites, ISPs also use other less transparent methods,

28 "Banistan: Why Is YouTube Still Blocked In Pakistan?" *New Yorker*, August 7, 2013, http://nyr.kr/1WS2dtH.

29 Mehtab Haider, "PTA may be empowered to undertake Internet content management," *The News*, February 22, 2015, http://bit.ly/1R2KLyZ.

30 Mehtab Haider, "PTA given powers for content management on internet," *The News*, March 21, 2015, http://bit.ly/1ED2NjN.

31 Article 19, "Pakistan: Telecommunications (Re-organization) Act."

32 "Pakistan: Code of Criminal Procedure," available at the Organization for Economic Co-operation and Development, accessed August 2013, http://bit.ly/1R2Kyfg.

33 PTA Act 1996, art. 23.

34 Danny O'Brien, "Pakistan's Excessive Internet Censorship Plans," Committee to Protect Journalists (blog), March 1, 2012, https://cpj.org/x/4995.

35 National ICT Research and Development Fund, "Request for Proposal: National URL Filtering and Blocking System," accessed August 2012, http://bit.ly/1QeBBiD; "PTA determined to block websites with 'objectionable' content," *The Express Tribune*, March 9, 2012, http://bit.ly/xEND9P.

36 Shahbaz Rana, "IT Ministry Shelves Plan to Install Massive URL Blocking System," *The Express Tribune*, March 19, 2012, http://bit.ly/1MilIIQ.

37 Anwer Abbas, "PTA, IT Ministry at Odds Over Internet Censorship System," *Pakistan Today*, January 3, 2013, http://bit.ly/1N47IkG; ApurvaChaudhary, "Pakistan To Unblock YouTube After Building Filtering Mechanism," *Medianama*, January 10, 2013, http://bit.ly/TMmcvh; Abdul Quayyum Khan Kundi, "The Saga of YouTube Ban," Pakistan Press Foundation, January 2, 2013, http://bit.ly/1bhpMEP; "Ministry Wants Treaty, Law to Block Blasphemous Content," *The News*, March 28, 2013, http://bit.ly/16JP6yo. Associated Press of Pakistan, "IT Minister plans to ban 'objectionable content' across entire internet," *The Express Tribune*, http://bit.ly/1VJApFx.

38 Senft, et al., *O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Net sweeper's Role in Pakistan's Censorship Regime.*

such as DNS tampering," Citizen Lab noted. [39] The report highlighted the lack of transparency and accountability surrounding censorship in Pakistan.

The same lack of transparency extends to the content affected by censorship, which is often inconsistent based on location or across ISPs.[40] There are no published guidelines outlining why content is blocked or how to appeal. Individuals and groups can also initiate censorship by petitioning courts to enact moral bans on online or traditional media content.[41] In April 2016, attempts to access the website of the French satirical magazine *Charlie Hebdo* from within Pakistan prompted the message, "Surf Safely! The website is not accessible. The site you are trying to access contains content that is prohibited for viewership within Pakistan as per the law." The magazine is known for mocking religion and was attacked by extremists in January 2015.

Blocking frequently targets social media and communication apps. In 2012, the government blocked YouTube in response to the anti-Islamic video "The Innocence of Muslims."[42] The site was briefly unblocked in December 2012 until a broadcast journalist demonstrated that the offensive clip was still available, [43] and it remained off limits for users in Pakistan until this year. In January 2016, a localized version of the platform, YouTube PK, became accessible.[44] A government statement about the new platform said that "Google has provided an online web process through which requests to blocking access of offending material can be made by the PTA to Google directly." YouTube said that the company may remove content from local versions of its platforms based on local laws after a thorough review.[45]

No other applications were subject to deliberate blocking at the domain level during the coverage period. Pakistani users of WhatsApp, the widely-used instant-messaging service owned by Facebook, could not connect to the service's iOS or Android apps for a brief period on May 18, 2016, but it is not known what caused the outage.[46]

Censorship targeting pornography can affect access to health information and other legitimate content like Scarleteen, a U.S.-based sex education website for teenagers.[47] In January 2016, the PTA informed internet service providers that 429,343 websites must be blocked at the domain level,[48] in an attempt to prevent access to pornographic sites. The manner in which the list of websites has been vetted to avoid non-pornographic websites from being blocked has not been made clear to the public.

Political dissent and secessionist movements in areas including Baluchistan and Sindh province, where a Sindhi nationalist movement advocates for political divisions along ethnic lines, is among the nation's most systematically censored content.[49] In 2013, the PTA requested that ISPs block the

39 DNS tampering intercepts the user's request to visit a functioning website and returns an error message.

40 OpenNet Initiative, "Country Profile—Pakistan," 2012.

41 "Internet censorship: Court asked to ban inappropriate content," *The Express Tribune*, June 14, 2011, http://bit.ly/jOCZFP.

42 Jon Boone, "Dissenting voices silenced in Pakistan's war of the web," *The Guardian*, February 18, 2015, http://gu.com/p/45yba/stw.

43 Umar Farooq, "Pakistan Courts YouTube Comeback," *Wall Street Journal,* August 14, 2013, http://on.wsj.com/1jiCfkv.

44 Requests to access Youtube.com redirect users within Pakistan to youtube.com/?hl=ur&gl=PK

45 "Pakistan lifts three-year YouTube ban with censor-friendly version", *Newsweek*, January 19, 2016 http://bit.ly/1WSumCK.

46 "After Brief Outage, Whatsapp Services Restored in Pakistan", ProPakistani, May 18, 2016, http://bit.ly/28IeLoN

47 "Pakistan blocks access to teen sex-ed site," *The Express Tribune*, March 20, 2012, http://bit.ly/1QeD0pE.

48 " Pakistan to block over 400,000 porn websites", *The Express Tribune*, January 26, 2016 http://bit.ly/1TIIsGk.

49 "PTA letter blocking websites April 25, 06," *Pakistan 451* (blog), April 27, 2006, http://bit.ly/1Lmn18M.

international website IMDb (Internet Movie Database), an order they reversed after two days.[50] Analysts said the apparent ban—which attracted widespread criticism on social media—was related to the upcoming release of a British short film, "The Line of Freedom," a fictional depiction of Pakistani security agencies abducting Baloch separatists. [51] The IMDb page documenting "The Line of Freedom" remained inaccessible for longer, but it was also ultimately unblocked.[52]

Authorities also target users seeking to access blocked content. In 2011, the PTA sent a legal notice to all ISPs in the country urging them to report customers using encryption and virtual private networks (VPNs)[53] —technology that allows internet users to interact online undetected and access blocked websites—to curb communication between terrorists.[54] International and civil society organizations in Pakistan protested,[55] and the tools were widely used to access YouTube when it was blocked.[56] Two of the best-known services, Spotflux and HotSpot VPN, became inaccessible in 2014, and Spotflux said the government had actively blocked its services.[57] Both were later restored.

Content Removal

State and other actors are known to exert extralegal pressure on publishers and content producers to remove content, but it frequently goes unreported. Takedowns by international companies are more high profile. Facebook reported restricting 6 items "that were alleged to violate local laws prohibiting blasphemy" in the second half of 2015.[58]

Official requests to remove content generally lack transparency. Following a major terrorist attack in December 2014, the government ordered material published by banned terrorist outfits to be removed from the internet, though published reports did not elaborated on the process involved.[59]

Media, Diversity, and Content Manipulation

Despite existing limitations on online content—and looming new ones—Pakistanis have open access to international news organizations and other independent media, as well as a range of websites representing Pakistani political parties, local civil society groups, and international human rights organizations. [60] ICTs, particularly mobile phones, promote social mobilization. After YouTube was

50 "Climbdown: PTA restores IMDb access after public outcry," *The Express Tribune*, November 23, 2013, http://bit.ly/1R2MVyv;Nighat Dad, "Why was IMDb blocked?" *The Express Tribune*, November 23, 2013, http://bit.ly/1QeE3Wz.

51 IMDb, "The Line of Freedom," http://www.imdb.com/title/tt2616400/.

52 Digital Rights Foundation, "First Case of Selective / Targeted Online Censorship: Pakistani Government Successfully Blocks Specific Links," press release, November 25, 2013, http://bit.ly/1Lmnjg7.

53 Josh Halliday and Saeed Shah, "Pakistan to ban encryption software," *The Guardian*, August 30, 2011, http://bit.ly/outDAD.

54 Nighat Dad, "Pakistan Needs Comms Security Not Restrictions," Privacy International (blog), September 12, 2011, http://bit.ly/1QeEvEi.

55 Barbora Bukovska, "Pakistan: Ban on internet encryption a violation of freedom of expression," Article 19, September 2, 2011, http://bit.ly/1Mlv3ja.

56 The VPN blocking is authorized under section 5(2)(b) of the PTA Act 1996 and the "Monitoring and Reconciliation of Telephony Traffic Regulation. See, "Part II, S.R.O. Pakistan Telecommunication Authority Notification," *The Gazette of Pakistan*, March 15, 2010, http://bit.ly/1Lby01z.

57 "Creeping censorship: Spotflux claims its service is being 'actively blocked' in Pakistan," *The Express Tribune,* January 28, 2014, http://bit.ly/1dK9W3U.

58 "Governmen Requests Report for Pakistan", Facebook, https://govtrequests.facebook.com/country/Pakistan/2015-H2/.

59 "Govt directs PTA to remove banned outfits' hate-material from internet, *"Dunya News*, 16 January 2015, http://bit.ly/1huNqoR

60 OpenNet Initiative, "Country Profile—Pakistan," 2012.

unblocked, all social networking, blogging, and VoIP applications were available and widely used during the coverage period. Nevertheless, most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, and women's and LGBTI (lesbian, gay, bisexual, transgender, and intersex) rights.

Digital Activism

Human rights activists have galvanized public support against militancy using digital technology. In December 2014, when an influential cleric in Islamabad refused to categorically condemn a terrorist attack on a school, activists gathered outside the cleric's mosque, demanding an apology for the previous statement.[61] The call to protest originated through social media and text messages using the #ReclaimYourMosque hashtag.[62] A Taliban spokesman contacted the protest organizer, threatening him to back off or "be ready for consequences."[63]

The coverage period saw a continuation of the fight by rights organizations in Pakistan against the Prevention of Electronic Crimes Bill, using hashtags like #MyLifeAfterPECB and #PakRejectsCyberBill to raise awareness of threats to digital rights in the draft (see Legal Environment).

Violations of User Rights

Violations of user rights continued at high levels during the coverage period, including two 13-year prison sentences handed down by antiterrorism courts for content shared on Facebook. Civil society groups say the Prevention of Electronics Crimes Act approved in 2016 criminalizes legitimate online activity. Researchers uncovered compelling information about Pakistani agencies' surveillance ambitions and capabilities during the coverage period.

Legal Environment

Article 19 of the Pakistani constitution establishes freedom of speech as a fundamental right, although it is subject to several restrictions.[64] Pakistan became a signatory to the International Covenant on Civil and Political Rights in 2010.[65]

Several laws have the potential to restrict internet users. The 2004 Defamation Act allows for imprisonment of up to five years, and observers fear a chilling effect if it is used to launch court cases for online expression. Section 124 of the penal code on sedition "by words" or "visible representation" is broadly worded, though it has yet to be applied in an online context.[66]

Section 295(c) of the penal code, which covers blasphemy, is frequently invoked to limit freedom of expression. Any citizen can file a blasphemy complaint against any other, and human rights groups say charges have been abused in the past to settle personal vendettas. The imputation of blasphemy

61 Ikram Junadi, "Islamabad stands firm on Lal Masjid," *Dawn,* December 20, 2014, http://www.dawn.com/news/1151985.
62 Ikram Junadi, "Citizens arrive at Lal Masjid to 'reclaim their mosque'," *Dawn*, December 19, 2014, http://bit.ly/1v7dPtz.
63 "Lal Masjid protest activist receives threatening phone call," *Dawn*, December 22, 2014, http://www.dawn.com/news/1152467.
64 The Constitution of Pakistan, accessed September 2012, http://bit.ly/pQqk0.
65 "President signs convention on civil, political rights," *Daily Times*, June 4, 2010, http://bit.ly/1fyK9TI.
66 "Pakistan Penal Code," accessed August 2013, http://bit.ly/98T1L8.

leaves the accused vulnerable to reprisals, regardless of whether it has foundation. Many cases have involved electronic media (see Prosecutions and Detentions for Online Activities).

Laws to combat terrorism can also been exploited against internet users. The Pakistan Protection Act passed in July 2014, reformulating a problematic Pakistan Protection Ordinance. Despite the reformulation, critics said it failed to address concerns expressed by lawyers and civil society groups, who said language categorizing unspecified cybercrimes as acts of terror was vague and open to abuse.[67]

The National Assembly approved the Prevention of Electronics Crimes Act during the coverage period of this report; at the end of the coverage period, it was pending Senate approval.[68] It passed in August 2016. Observers reported that the drafting process lacked transparency. The National Standing Committee on Information Technology and Telecommunication held a hearing to discuss the bill in May 2015, which included some criticism from civil society. But no major changes were incorporated in the version which the committee subsequently approved in September, and some committee members said they had not even been allowed to read it.[69] That draft was rejected by the Senate. In April 2016, an amended version of the bill was put forward again, and approved by the National Assembly.[70] Although the amended bill was approved on April 13, it was not released to the public until May 7,[71] though an unofficial copy was leaked to journalists.[72]

Though it contained some procedural safeguards for cybercrime investigations by law enforcement agencies, international and local human rights groups condemned the Act's overly broad language and disproportionate penalties, including 14 year prison terms for acts of cyberterrorism that the law failed to adequately define.[73] The law also punishes preparing or disseminating electronic communication to glorify terrorism; and preparing or disseminating information that is likely to advance religious, ethnic or sectarian hatred, both with up to seven years in prison. Section 18 criminalizes displaying or transmitting information that intimidates or harms the "reputation or privacy of a natural person" with a maximum three year prison term or a fine of PKR 1 million (US$9,500) or both.[74] Other problematic features of the include Section 37, which grants the PTA broad censorship powers (see Blocking and Filtering), and other sections governing officials' access to data (see Surveillance, Privacy, and Anonymity).

The Surveying and Mapping Act 2014 limits digital mapping activity to organizations registered with the governmental authority Survey of Pakistan, with federal permission required for mapping collab-

67 Bolo Bhi, "Human Rights Experts: Pakistan Could Become a "Police State" Under Protection Ordinance," *Global Voices Advocacy*, August 13, 2014, http://bit.ly/1OqLFGd.

68 "Cybercrime bill relegated to yet another committee", Dawn, June 23, 2016, http://www.dawn.com/news/1266681/

69 Fazal Sher, "Absence of comprehensive law against cybercrimes: NR3C of FIA unable to take action against criminals," *Business Recorder*, February 10, 2015, http://bit.ly/1PlaioF; Digital Rights Foundation, "Standing Comm. Passes Draft of PECB, Unseen by Comm. Members," September 21, 2015, http://bit.ly/1QeGTuA.

70 "Controversial Cyber Crime Bill approved by NA" Dawn, April 13, 2016 http://www.dawn.com/news/1251853

71 "The Peculiar timing of NA's decision to release Cyber Crime Law's final draft", Digital Rights Foundation, May 7, 2016, http://bit.ly/28BaVna.

72 APC Impact, "Deconstructing Prevention of Electronic Crimes Bill 2015 – "Chapter II Offences and Punishments" – Part 1," April 18, 2015, http://www.netfreedom.pk/deconstructing-prevention-of-electronic-crimes-bill-2015-chapter-ii-offences-and-punishments-part-1/.

73 Digital Rights Foundation, "The Prevention of Electronic Crimes Bill 2015 - An Analysis," June 2016, https://www.article19.org/data/files/medialibrary/38416/PECB-Analysis-June-2016.pdf.

74 Prevention of Electronic Crimes Bill, accessible: http://digitalrightsfoundation.pk/wp-content/uploads/2016/08/PECB2016.pdf.

oration with foreign companies.[75]

Prosecutions and Detentions for Online Activities

Electronic speech perceived as blasphemous has been prosecuted in the past several years in Pakistan. In a new development during the coverage period, individuals were sentenced to 13 years in prison in two separate cases for allegedly distributing "hateful" or "sectarian" material on Facebook. Though little is known about the details of the cases, neither was publicly reported to involve threats of violence. The secrecy surrounding verdicts apparently penalizing online speech was concerning. In both instances, the men were tried and sentenced by Pakistani antiterrorism courts, rather than civil or criminal courts.[76] Antiterrorism courts were established under the Anti-Terrorism Act passed in 2007 and repeatedly amended to cover more offenses. They have been criticized for violating human rights, since trials take place behind closed doors and defendants are denied a full defense and the presumption of innocence.[77]

In November 2015, an antiterrorism court in Lahore sentenced a man belonging to the Shia sect of Islam to 13 years in prison and a fine of PKR 250,000 (US$2,400) under the antiterrorism act for posting "sectarian hate speech" characterized as "against companions of the Prophet of Islam" on Facebook, according to international news reports citing local officials.[78] Local digital rights group Bytes for All said they had not been able to independently verify the details of the case.[79]

In March 2016, in a separate case, another Shia man was sentenced to 13 years in prison and a fine of PKR 250,000 (US$2,400), also by an antiterrorism court in Lahore, on three counts of promoting sectarian hatred on Facebook. His lawyer told Agence France-Presse that he was not responsible for distributing the content, but had only "liked" it on Facebook. The public prosecutor described the post as being "against the belief of Sunni Muslims," according to Agence France-Presse.[80]

On June 8, 2016, the Supreme Court granted bail to two women from Rawalpindi who had been detained for two months for allegedly sharing "vulgar pictures and defamatory text messages."[81] Some news reports said they had sent the messages to another woman, but at least one reported they had tampered with images of a female relative and distributed them on WhatsApp.[82] The Islamabad High Court had rejected initial pleas for bail. News reports said they were charged under Sections 36 and 37 of the Electronic Transaction Ordinance of 2002, which punish "violations of privacy of information" and "damage to information systems" respectively.

75 Nighat Dad, "Pakistan Considering Bill that Would Ban Independent Mapping Projects," Tech President, November 28, 2012, http://bit.ly/1OpVqpK; Pakistan National Assembly, Bill to provide for constitution and regulation of Survey of Pakistan, No. 225/25/2012, November 14, 2012, http://bit.ly/1OpVwOc.

76 Agence France-Presse, 25-year-old sentenced to 13 years in prison over 'religiously offensive' Facebook post," via *Express Tribune,* March 3, 2016, http://tribune.com.pk/story/1058813/25-year-old-jailed-for-13-years-over-facebook-post/.

77 Huma Yusuf, "Pakistan's Anti-Terrorism Courts," *CTC Sentinel,*March 3, 2010, https://www.ctc.usma.edu/posts/pakistan%E2%80%99s-anti-terrorism-courts.

78 Press Trust of India, "Pak sentences man to 13 years in jail for FB hate speech," *Business Standard,* November 24, 2015, http://www.business-standard.com/article/pti-stories/pak-sentences-man-to-13-years-in-jail-for-fb-hate-speech-115112400011_1.html.

79 "Pakistani Shia man jailed for 13 years for Facebook 'hate speech'", Dawn November 24, 2015, http://www.dawn.com/news/1221725.

80 Agence France-Presse, 25-year-old sentenced to 13 years in prison.

81 "SC grants bail to two women jailed for sending 'vulgar' texts" Express Tribune, June 9, 2016 http://bit.ly/24NZ8Nv

82 Shahid Rao, "Bail pleas of victim's in-laws rejected," *The Nation,* April 29, 2016, http://nation.com.pk/islamabad/29-Apr-2016/bail-pleas-of-victim-s-in-laws-rejected.

On October 28, 2015, Pakistan's Federal Investigation Agency arrested an activist and member of the Pakistan Tehreek-i-Insaf political party for comments posted on Twitter in September. The comments, which pertained to relatives of a member of the judiciary presiding over a corruption case, have since been deleted.[83] The activist, Jalal Qazi, was also charged with violating clauses 36 and 37 of the Electronic Transaction Ordinance. Each clause carries a maximum seven year jail term, fines up to PKR 1 million rupees, or both."[84] He was released on bail on November 3, 2015.[85]

Fresh blasphemy accusations were reported during the coverage period, but had not gone to trial in mid-2016. On May 25, 2016, a Christian man, named in reports as Usman Masi, was charged by police in Sheikhupura, with allegedly posting "blasphemous" material on an unspecified social media website.[86] He was not reported to be in custody.

Surveillance, Privacy, and Anonymity

The Prevention of Electronics Crimes Act passed after the coverage period of this report, granted overly broad surveillance powers, both to agencies within Pakistan, and potentially beyond, since it includes provisions that permit the sharing of data with international agencies without adequate oversight.[87]

A 2007 Prevention of Electronic Crimes Ordinance requiring telecommunications companies to retain user traffic data for a minimum of 90 days, and share logs of customer communications with security agencies when directed by the PTA, expired in 2009, though the practices reportedly continued.[88] The Prevention of Electronic Crimes Act retained the 90-day minimum, and allows an "authorized officer" to request extended data retention without oversight. The PECB also grants "authorized officers" to request that users hand over their decryption keys (if the data is encrypted), or else face prosecution.[89]

Government surveillance was already a concern for activists, bloggers, and media representatives, as well as ordinary internet users. Pakistani authorities, particularly intelligence agencies, appear to have been expanding their monitoring activities in recent years, while provincial officials have been exerting pressure on the central government to grant local police forces greater surveillance powers and location tracking abilities, ostensibly to curb terrorism and violent crimes.[90]

In 2015, an investigation by U.K.-based Privacy International revealed that the government's surveillance capability, particularly that of the Inter-Services Intelligence Agency, outstrips domestic and

83 "Qazi Jalal arrested in Peshawar for a Tweet", Teeth Maestro Blog, October 28, 2015, http://bit.ly/1ttMCaL.

84 "Can a Tweet get you arrested in Pakistan? Yes, it can", Express Tribune, October 29, 2015 http://bit.ly/1RhJ018.

85 "FIA arrests PTI's social media member over violation of cyber laws", The News, October 29, 2015 http://bit.ly/1Tzkso6.

86 "Christian man booked for posting blasphemous text on social media" May 26, 2016, http://bit.ly/21jJg0d.

87 Data includes the "communication's origin, destination, route, time, data, size, duration or type of underlying service." See, Nighat Dad, Adnan Chaudhri, "The Sorry Tale of the PECB, Pakistan's Terrible Electronic Crimes Bill" Digital Rights Foundation, November 26, 2015, http://bit.ly/1WcxTwb.

88 Kelly O'Connell, "INTERNET LAW – Pakistan's Prevention of Electronic Crimes Ordinance, 2007," *Internet Business Law Services*, http://bit.ly/1NvN1kw.

89 "A Deeper Look Inside the PECB, Pakistan's Terrible Cyber-Crime Bill", Electronic Frontier Foundation, November 30, 2015 http://bit.ly/24lAjtW.

90 Masroor Afzal Pasha, "Sindh Police to Get Mobile Tracking Technology," *Daily Times*, October 29, 2010, http://bit.ly/16TKfLY; "Punjab Police Lack Facility of 'Phone Locator', PA Told," *The News*, January 12, 2011, http://bit.ly/1bRl6bx.

international law regulating that surveillance.[91] "Mass network surveillance has been in place in Pakistan since at least 2005," using technology obtained "from both domestic and foreign surveillance companies, including Alcatel, Ericsson, Huawei, SS8 and Utimaco," according to the report.

A report released in 2013 by Citizen Lab indicated that Pakistani citizens may be vulnerable to oversight through a software tool present in the country. FinFisher's "Governmental IT Intrusion and Remote Monitoring Solutions" package includes the FinSpy tool, which attacks the victim's machine with malware to collect data including Skype audio, key logs, and screenshots. [92] The analysis found FinFisher's command and control servers in 36 countries worldwide, including on the PTCL network in Pakistan. This did not confirm that actors in Pakistan are knowingly taking advantage of its capabilities. In 2014, however, hackers released internal FinFisher documents indicating that a client identified as "Customer 32" licensed software from FinFisher to infect Microsoft office documents with malware to steal files from target computers in Pakistan.[93]

In July 2015, data belonging to Italian commercial digital surveillance company Hacking Team was leaked online by hackers, revealing communications between senior Hacking Team personnel and private-sector representatives of foreign intelligence agencies. In the case of Pakistan, these communications went back to 2011, and documented meetings with intelligence agents, and requests for mobile interception technologies. No purchases were reported. [94]

Official agencies also use less covert means to obtain user data. According to the most recent transparency reports, Twitter received one specific account request from the Pakistani government between July 2015 and December 2015. [95] Facebook reported nearly 500 user data requests by the Pakistani government during the same period, of which 66 percent led to "some data...produced."[96]

In July 2015, the government instructed Blackberry to allow officials access to encrypted messages sent through the company's servers or discontinue operating in Pakistan.[97] In December, the company reported it had been allowed to continue operating even though it had not complied.[98]

The Fair Trial Act, passed in 2013, [99] allows security agencies to seek a judicial warrant to monitor private communications "to neutralize and prevent [a] threat or any attempt to carry out scheduled offences." It covers information sent from or received in Pakistan, or between Pakistani citizens whether they are resident in the country or not. Under the law, service providers face a one-year jail term or a fine of up to PKR 10 million (US$103,000) for failing to cooperate with warrants. Warrants can be issued if a law enforcement official has "reason to believe" in a terrorism risk; it can also be temporarily waived by intelligence agencies. A 2014 white paper issued by the Digital Rights Group said

91 Matthew Rice, "Tipping the Scales: Security and surveillance in Pakistan," Privacy International, July 21, 2015, https://www.privacyinternational.org/node/624.

92 Morgan Marquis-Boire et al, *For Their Eyes Only: The Commercialization of Digital Spying*, Citizen Lab, May 1, 2013, http://bit.ly/ZVVnrb.

93 Sohail Abid, "Massive Leak Opens New Investigation of FinFisher Surveillance Tools in Pakistan," Digital Rights Foundation, via Global Voices Advocacy, August 22, 2014, https://advox.globalvoices.org/2014/08/22/massive-leak-opens-new-investigation-of-finfisher-surveillance-tools-in-pakistan/.

94 Bolo Bhi, "Hacking Team in Pakistan," http://bolobhi.org/hacking-team-in-pakistan/.

95 "Transparency Report" for Pakistan, Twitter, accessed May 3 2016 https://transparency.twitter.com/country/pk

96 Government Requests Report for Pakistan", Facebook, https://govtrequests.facebook.com/country/Pakistan/2015-H2/.

97 BBC News, "Blackberry to keep operating in Pakistan," December 31, 2015, http://www.bbc.com/news/technology-35204922.

98 Marty Beard, "Continuing our Operations in Pakistan," December 31, 2015, *Inside Blackberry,* http://blogs.blackberry.com/2015/12/continuing-our-operations-in-pakistan/.

99 "Investigation for Fair Trial Act 2013," *The Gazette of Pakistan,* February 22, 2013, http://bit.ly/18esYjq.

that provisions of the Fair Trial Act contravene the Constitution and international treaties Pakistan has signed in the past.[100]

ISPs, telecommunications companies, and SIM card vendors are required to authenticate the Computerized National Identity Card details of prospective customers with the National Database Registration Authority before providing service.[101] A registration drive was launched following a December 2014 attack on a school that dozens of students. Investigators tracked three unregistered SIM cards used by the terrorists for communication during the attack.[102] Following the attack, the government required citizens to verify numbers registered against their names and added a biometric thumb impression to SIM card registration requirements.[103] In 2015, SIM card owners without biometric identification were warned of automatic disconnection, and 26 million SIM cards were subsequently disconnected or blocked.[104]

Pakistanis are also vulnerable to surveillance from overseas intelligence agencies. In June 2015, digital security and intelligence magazine *The Intercept* published revelations of hacking and infiltration of the Pakistan Internet Exchange (PIE) by Britain's GCHQ intelligence agency prior to 2008. According to *The Intercept*, this gave GCHQ "access to almost any user of the internet inside Pakistan" and the ability to "re-route selected traffic across international links towards GCHQ's passive collection systems."[105]

Intimidation and Violence

Pakistan is one of the world's most dangerous countries for traditional journalists.[106] Online journalists can also be vulnerable.

Violence against women thought to have brought shame on their communities—including murder via "honor killings"—has begun to involve ICT usage. In April 2016, a 16-year old girl was killed by her older brother for using a mobile phone.[107]

Leaking explicit photos, threats of blackmail, and other incidences of online harassment are increasing in Pakistan. More than three thousand cybercrimes were reported to the Federal Investigation Agency from August 2014 to August 2015.[108] Of those cases, 45 percent targeted women on social

100 "Privacy rights: Whitepaper on surveillance in Pakistan presented," *The Express Tribune*, November 16, 2014, http://bit.ly/1L4h8Mc; Waqqas Mir, et al. "Digital Surveillance Laws in Pakistan," eds. Carly Nyst and Nighat Dad, (a white paper by Digital Rights Foundation, November 2011) http://bit.ly/1jg2IzH.

101 Bilal Sarwari, "SIM Activation New Procedure," *Pak Telecom*, September 3, 2010, http://bit.ly/pqCKJ9.

102 Akhtar Amin, "PTA fails to block unregistered SIMs despite court orders," *The News*, December 26, 2014, http://bit.ly/1P4zSyZ.

103 Ahmad Fuad, "Biometric SIM verification: a threat or opportunity for cellular firms?" *The Express Tribune*, February 1, 2015, http://bit.ly/1LbAtJe.

104 Aamir Attaa, "Biometric Verification of SIMs is not Fool Proof: Chairman PTA," ProPakistani, March 16, 2015, http://bit.ly/1QeImAZ; "26 million SIMs Blocked As SIM Reverification Drive Ends, ProPakistani, April 13, 2015 http://bit.ly/24Bm5VT.

105 "Spies Hacked Computers Thanks To Sweeping Secret Warrants, Aggressively Stretching UK Law", The Intercept, June 22, 2015, http://bit.ly/1VMfTZN.

106 Committee to Protect Journalists, "56 Journalists Killed in Pakistan since 1992/Motive Confirmed," accessed January 2014, http://bit.ly/1LE6kYI.

107 Chris Summers, "Man stabs his 16-year-old sister to death in Pakistan 'honour killing' - because she was using a mobile phone," *Daily Mail,* April 28, 2016, http://www.dailymail.co.uk/news/article-3563679/Pakistan-police-arrest-man-honour-killing-sister.html.

108 Noorwali Shah, "In the cyberspace: Technology illiteracy leads to online harassment," *The Express Tribune*, August 12, 2015, http://bit.ly/1N4gWgJ.

media. The figures only represent reported cases—many victims do not come forward for fear of losing access to ICTs. No data has been provided for other provinces.

Militant Islamic groups have launched attacks on cybercafes and mobile phone stores in the past for allegedly encouraging moral degradation.[109] No attacks were documented during the coverage period of this report.

Free expression activists and bloggers have also reported receiving death threats. Many publicize the threats—and sometimes attract more—on Twitter. Most are sent via text message from mobile phones, often originating from the tribal areas of the country, and several include specific details from the recipient's social media profiles or other online activity.

Technical Attacks

Technical attacks against the websites of nongovernmental organizations, opposition groups, and activists are common in Pakistan but typically go unreported due to self-censorship, and were not publicized during the coverage period. The websites of government agencies are also commonly attacked, often by ideological hackers attempting to make a political statement.[110] In 2015, the website of the religious political party Jamaat-e-Islami was hacked for its alleged support of terrorists.[111]

Officials allege that most cyberattacks originate in India; groups based in Pakistan also hack Indian websites.[112]

109 "Blast in Nowshera destroys internet cafe, music store," *Dawn*, February 2, 2013, http://bit.ly/1jiOhdA; "Fresh Bomb Attacks Kill 2 Shias, wound 20 in Pakistan," *Press TV,* January 13, 2013, http://bit.ly/Ssoth2; Associated Press, "Police: Bomb Blast at Mall in Northwestern Pakistan Kills 1 Person, Wounds 12," *Fox News*, February 21, 2013, http://fxn.ws/YI5QCq.

110 Hisham Almiraat, "Cyber Attack on Pakistan's Electoral Commission Website," *Global Voices Advocacy*, April 1, 2013, http://bit.ly/1WSbWQL.

111 Usman Khan, "Jamaat-e-Islami website hacked over 'alleged support for terrorism," *The News Tribe,* January 20, 2015, http://bit.ly/1P4CvB5.

112 "Cybercrimes: Pakistan lacks facilities to trace hackers," *The Express Tribune*, February 1, 2015, http://bit.ly/1FWXTW7.