Pakistan

Not Free

26

100

A **Obstacles to Access** 5 25
B **Limits on Content** 14 35
C **Violations of User Rights** 7 40

Last Year's Score & Status

27 100 Not Free

**Overview**

Internet freedom declined during this report’s coverage period due to authorities’ increased blocking of political, social, and cultural websites. The general election environment in July 2018 saw connectivity restrictions and increased disinformation. Meanwhile, authorities upped their efforts to silence critical journalists and activists using a range of techniques. Users were again sentenced to death on charges of posting blasphemous content online, although their convictions are under appeal.

Pakistan holds regular elections under a competitive multiparty political system.
However, the military exerts enormous influence over security and other policy issues, intimidates the media, and enjoys impunity for indiscriminate or extralegal use of force. The authorities impose selective restrictions on civil liberties, and some Islamist militant groups carry out attacks on religious minorities and other perceived opponents.

**Key Developments**

**June 1, 2018 - May 31, 2019**

- Authorities shut down mobile and internet service during protests and in the lead-up to the July 2018 general elections, in both populous cities and less developed regions (see A3 and B8).

- Over 800,000 websites are blocked, including political, religious, and social content. Voice of America’s websites in Urdu and Pashto were temporary inaccessible during the coverage period, as was the website of the leftist Awami Workers Party (see B1).

- Inauthentic content and automated accounts impacted the online landscape. Bots supporting various political parties surfaced ahead of the July 2018 general elections, while Facebook remove content it claimed to be linked to the Pakistani military’s public relations department (see B5).

- In December 2018, two brothers were sentenced to death for blasphemy, for allegedly sharing “disrespectful material” about the prophet Mohammad on their website in 2011 (see C3).

- The government increased social media monitoring, announcing a new system to target extremism, hate speech, and antinational content. The announcement came a month before the Interior Ministry launched an investigation into journalists and activists supporting murdered journalist Jamal Khashoggi on social media (see C5).
• Activists and bloggers faced physical attacks and death threats during the coverage period. Social media activist and Waqt TV journalist Gul Bukhari was abducted by unknown persons and returned a few hours later in June (see C7).

A Obstacles to Access

Underdeveloped infrastructure limits internet penetration rates in Pakistan, particularly in rural areas. However, mobile internet access is increasing. Pakistani authorities frequently disable internet access during times of perceived unrest; meanwhile, already long-term denial of service in marginalized areas persisted during the coverage period.

A1 0-6 pts
Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

Internet penetration registered only marginal increases during the reporting period. There are 67 million broadband connections in Pakistan, an increase of 10 million since the last report.1 A majority of internet subscribers come from mobile broadband and 3G and 4G internet.2 The Inclusive Internet Index 2019, a publication of the Economist, ranked Pakistan at 84 out of 100 in terms of availability, determined by quality and breadth of available infrastructure.3 According to the most recent data available from the International Telecommunications Union (ITU), just under 16 percent of Pakistani residents accessed the internet in 2017.4

The speed-testing company Ookla ranked Pakistan’s mobile broadband download speed at 14.03 Mbps in mid-2018.5 Infrastructural limitations are acute in rural localities, limiting broadband access.

Damaged or inadequate infrastructure also periodically disrupts access, although there were no major internet disruptions due to infrastructural issues during the coverage period, as there had been in 2017.6 In August of that year, damage to an international submarine cable system, I-ME-WE (India-Middle East-Western Europe), led to a nationwide disruption in service for approximately 48 hours.7 Customers
reported slow internet speeds in August 2018,8 as another international cable system, SEA-ME-WE 4 (Southeast Asia-Middle East-Western Europe 4), that is key to internet access in Pakistan, was under repair; the disruption highlighted the need for diversified internet infrastructure.

Power outages are a serious problem in Pakistan, and also limit connectivity.9

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?

There are serious inequalities in access to information and communications technology (ICTs) based on geographic location, gender, and socioeconomic status.

While the cost of internet has fallen considerably in the last few years, access remains out of reach for the majority of the population, and high taxes on internet service push prices higher. Pakistan ranked 47 out of 100 countries surveyed in the Inclusive Internet Index 2019 report’s affordability index, which examines cost of access relative to income and the level of competition in the internet marketplace. The country ranked at 67 for price alone.

The affordability and taxation of telecommunications has been a source of public debate and legal wrangling. In June 2018, the Supreme Court of Pakistan suspended all taxes collected by telecommunications companies from their customers. However, in April 2019, the Supreme Court overturned the ruling and thus reinstated the tax. While the ruling was in effect and customer-paid taxes were suspended—from July 2018 until January 2019—the Federal Board of Revenue reported a slight fall in tax collection from telecommunication services.

Mobile phones were still taxed during this period, as Pakistan’s mini-budget, released in early 2019, imposed import duty taxes on phones that cost more than $350. This import tax considerably increased the price of mobile phones and prompted complaints among mobile service providers it resulted in a reduction in the number of people using 4G services.

Parts of western Pakistan lack internet access, in many cases due to underdevelopment or ongoing conflict. Areas in the former Federally Administered Tribal Areas (FATA) and Balochistan, for example, have difficult terrain, and a lack both of political will and of resources prevent infrastructural improvements. Smartphone penetration rates were estimated at 30 percent nationally in 2017; approximately 50 million people did not have mobile phones, according to the same study.

Government initiatives to provide access to remote areas have progressed in recent years. In 2017, the Punjab government installed 192 free internet hotspots Lahore, Rawalpindi, and Multan—though Pakistan’s poor record of protecting user privacy
may make some users reluctant to use them (see C5). In January 2018, it was announced that more than 10 billion Pakistani rupees ($81 million) worth of projects were to be launched, awarded by the Universal Service Funds (USF), to provide broadband service to remote areas, particularly Balochistan, Khyber Pakhtunkhwa, and the FATA region. Private investment is also moving into less connected areas; in October 2018, StormFiber announced that its Fiber to The Home (FTTH) infrastructure was expanding to the provincial capital of Quetta, in Balochistan.12

Low literacy, difficult economic conditions, and cultural resistance have also limited the proliferation of ICTs.13 The digital divide between men and women in Pakistan is among the highest in the world as a result of religious, social, and cultural restrictions on women owning devices.14 As per one study, Pakistani women are 43 percent less likely to use the internet than men.15 Even women who have access are likely to have their digital activities heavily monitored by family members and others. Women who are active online report high levels of online harassment that discourages greater utilization of ICTs (see C7).

A3 0-6 pts
Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?

Authorities frequently disrupt telecommunication services during protests, elections, and religious and national holidays, often citing security concerns. During the 2018 general elections, mobile internet services were notably suspended in parts of Balochistan, and in all of FATA during both the election period and the lead-up.

Frequent shutdowns continued throughout this report’s coverage period. In July 2018, mobile and internet services were shut down in parts of Lahore ahead of former prime minister Nawaz Sharif's return to Pakistan from London before the general elections, impeding rallies of supporters welcoming him back.1 In September, mobile services were suspended in Islamabad and other populous areas due to security concerns surrounding processions scheduled during the Ashura
In October, mobile networks were closed in Bannu in an attempt to thwart a peaceful protest organized by the Pashtun Tahafuz Movement (PTM), a grassroots civil rights movement. In November, mobile internet services were suspended in some parts of Sindh and Punjab on account of 12th Rabiul Awwal. Also in November 2018, mobile networks were shut down in all major cities during protests by right-wing groups that erupted after the Supreme Court acquitted Asia Bibi, a Christian woman accused of blasphemy.

During the coverage period, 3G, 4G, and LTE mobile internet services were also shut down in areas that receive comparatively little media attention, such as the less developed regions of Baluchistan, where several districts have had no mobile internet service since February 2017. While there has been no official justification for the shutdown, vague explanations based on national security grounds have been offered. Likewise, no deadline has been provided for restoration. A citizen challenged the shutdown at the Turbat bench of the High Court, but withdrew the case, reportedly after security officials pressured their lawyer to drop the matter. Long-term shutdowns have also been implemented in restive border regions, including one lasting more than three years in ex-FATA. In an encouraging development, mobile internet services were restored in Bajour in March 2019, after almost three years of restrictions.

In July 2018, just before the general election, the Ministry of Interior ordered that mobile internet be suspended in six districts of Balochistan, a move that effectively restricted the use of the Election Commission of Pakistan’s (ECP) mobile reporting mechanism. In November 2018, a parliamentary committee called on security agencies to review connectivity restrictions in the areas.

Section 54 of the 1996 Pakistan Telecommunications Act grants authorities the power to suspend services. While the law as written may only be invoked during a state of emergency, in practice it has been used to justify routine shutdowns, prompting a number of court cases.

In February 2018, the Islamabad High Court (IHC) held in a landmark ruling that mobile network shutdowns on the pretext of public safety under Section 54(3) of the PTA, including mobile-based internet suspension, infringed upon the fundamental rights of citizens and were thus illegal. However, in March 2018, the IHC suspended the judgment and the matter is still pending before the court. The IHC was originally hearing a separate petition challenging telecommunications
shutdowns during Pakistan Day celebrations.

The state exerts considerable influence over the internet backbone. 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, TW1.17

PTCL also controls access to three international undersea fiber-optic cables: SEA-ME-WE 3 (South-East Asia-Middle East -Western Europe 3) and SEA-ME-WE 4 connect Southeast Asia, the Middle East, and Western Europe; and I-ME-WE (India-Middle East-Western Europe) links India, the Middle East, and Western Europe.18 In July 2017, PTCL joined the AAE-1 (Asia-Africa-Europe-1) cable system. The 25,000-kilometer-long cable was built as part of China’s One Belt, One Road initiative and provides the lowest latency route to several countries across three continents.19 In February 2019, the Pak-China fiber optic, running from Rawalpindi to Khunjerab, became active.20 The project is owned by the military-run Special Communications Organization (SCO) and the contractor is Huawei. Internet rights groups have raised concerns regarding the dangers of a proposed terrestrial cable between Pakistan and China, given China’s highly restrictive internet model.21

- **2.** The Ashura holiday is observed most visibly by the Shiite sect, which is a minority group in Pakistan and often the target of sectarian terrorist groups. “Cellular networks jammed in different parts of country for 9, 10 Muharram,” Pakistan Today, last updated September 20, 2018, [https://www.pakistantoday.com.pk/2018/09/20/mobile-phone-service-suspen....](https://www.pakistantoday.com.pk/2018/09/20/mobile-phone-service-suspen....)


10. With the passage of the historic thirty-first amendment of the Constitution of Pakistan (Constitution (Thirty-First) Amendment Bill), passed by the National Assembly on May 24 2018. The FATA region is now part of the province of Khyber Pakhtunkhwa.


Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

Pakistan has a combination of private and publicly run service providers. During the coverage period, the state regulator abruptly raised operating fees for two major telecom service providers, prompting court cases that remain ongoing.

In 2019, abrupt changes to the telecom renewal policy threatened the ability of the two major telecom companies to operate. The licenses of Jazz and Telenor were set to expire on May 25, 2019. On May 9, the PTA released its Policy Directive for Renewal of Cellular Mobile Licenses 2019, which set the renewal fee at $450 million—nearly double the amount the operators paid in 2004 for licenses acquired at auction, to be paid by a new August 21 deadline. The telecoms in response brought a court challenge against the PTA. As of the beginning of September, the PTA accepted a payment of $224.6 million from each telecom for license renewal, but the legal cases continue.
According to licensing information published by the PTA, the government regulator, in 2018, there were 12 licensed wireless local loop (WLL) operators, 16 long distance and international (LDI) operators, and 21 operational fixed local loop (FLL) operators. Several dozen licenses had also been issued for companies, providing value-added services in the telecommunications sector. The PTA exerts significant control over internet and mobile providers through hefty licensing fees and various bureaucratic processes.

The predominantly state-owned PTCL has long dominated the broadband market. A Telecom Policy established in 2015 aimed to instill competitive practices in the telecom sector, though it led to overlapping regulatory powers for the Ministry of Information Technology and Telecom (MoITT) and the Competition Commission Pakistan (CCP).

There are four mobile operators in Pakistan. Pakistan Mobile Communications Limited (PMCL) is operated by its parent company VEON, which is headquartered in Amsterdam, and had a market share of 37 percent in 2019. It has begun merging the Mobilink and Warid brand names under the name Jazz to control the country's largest mobile subscriber base. Jazz's main competitors are Pak Telecom Mobile Limited (PTML), which is a PTCL subsidiary operating as Ufone (market share of 14 percent), Telenor Pakistan (market share of 27 percent), which is part of a Norwegian multinational company, and China Mobile Pakistan (CMPak), with a market share of 22 percent.


5. Wireless Local Loop (“WLL”) licenses are issued for the provision of fixed line telecommunication services within a Telecom Region using mediums including wireless, with limited mobility. See: “Master List of WLL Licensees for Pakistan,” Pakistan Telecommunication Authority, https://www.pta.gov.pk/assets/media/wll_list_140218.pdf.

6. Long Distance and International (LDI) licenses are issued for the provision of end to end communication between points that are located in Pakistan with points that are located outside of Pakistan. “LDI Operators for Pakistan,” Pakistan Telecommunication Authority, https://www.pta.gov.pk/media/ldi_lic_list_011117.pdf.

7. Fixed Local Loop (“FLL”) licenses are issued for the provision of fixed line telecommunication services within a Telecom Region using medium excluding wireless. See: “List of FLL Operators,” Pakistan Telecommunication Authority, https://www.pta.gov.pk/assets/media/ll_lic_250418.pdf.


10. 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.ca/2013/06/o-pakistan/.


A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

The PTA is the regulatory body for the internet and mobile industry, and internet
freedom advocates and human rights groups have expressed concerns about its lack of transparency and independence. ¹ The prime minister appoints the chair and members of the three-person authority, which reports to the MoITT. ²

The PTA plays an active role in implementing the various policies that undermine internet freedom. In March 2015, the PTA formally took responsibility for internet content management (see B3), this power was also consolidated in the Prevention of Electronic Crimes Act 2016 (PECA). However, there has been a lack of transparency and oversight of the PTA in terms of its decisions under section 37 of the PECA (see B3).


B Limits on Content

Social media platforms, communication tools, and other online tools are popular and contribute to a vibrant online space. However, online content is restricted by the Prevention of Electronic Crimes Act, which authorizes the PTA to undertake content management. Blocking of political content without transparency continued during the reporting period, including of websites relating to the general election. Disinformation and manipulated content continued to proliferate online, also ramping up around the vote.

B1 0-6 pts
Does the state block or filter, or compel service providers to block or filter, internet content?

Authorities frequently blocks political, religious, and social content critical of Islam or the military, sites that host pornography or nudity, and sites related to or offering circumvention and privacy tools, among others.¹ PTA figures reported in late 2018 show that at least 831,000 sites are blocked, including some 770,000 for pornographic content, 34,700 for blasphemy, at least 11,500 for antistate,
antijudiciary, or sectarian or hateful content, and more than 800 for defamation and/or impersonation.2

In June 2018, in the lead-up to the following month’s general elections, the website of the leftist Awami Workers Party (AWP) was blocked.3 It was restored after the party lodged objections with the Election Commission of Pakistan (ECP), but the PTA provided no explanation for the block. The party has petitioned the Islamabad High Court (IHC) about the case, which remains under consideration.4

In December 2018, it was reported that Voice of America’s (VOA) websites in Urdu and Pashto were inaccessible. A VOA official said that the Pashto-language website was blocked a few months prior, while the Urdu version was inaccessible after it reported on Mohsin Dawar, the leader of the Pashtun Tahafuz Movement (PTM).5 Both websites were eventually unblocked. Previously, in early 2018, a media blackout of PTM was ordered at the behest of the military establishment, and that April the news website NayaDaur was blocked in Pakistan for over a week before the PTA restored it. No reason for the blocking was provided by the government, but it followed its publication of an article sympathetic to the Pashtun human rights movement.6

During the coverage period, the government did not block social media or communication platforms, despite a threat from the Islamabad High Court warning that it might order the PTA to block Twitter for failing to remove content deemed “blasphemous.”7 Previously, in November 2017, social media applications and the websites of most news channels were blocked briefly throughout the country, due to what the government claimed were security concerns.

Political dissent and secessionist movements in areas including Balochistan and Sindh province have been subject to systematic censorship for years.8 In August 2016, the government banned websites operated by the Muttahida Qaumi Movement (MQM), a political party based in Sindh province, and said it would take steps to remove affiliated social media accounts after the party’s exiled leader delivered what officials and news reports characterized as an “anti-Pakistan” speech.9 The party’s official website remained blocked in mid-2019


B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?

State and other actors are known to exert extralegal pressure on publishers and content producers to remove content, and these instances frequently go unreported.

Pakistan is among the top countries where content is restricted on Facebook. Between July to December 2018, the number of content restrictions by Facebook doubled from 2,203 (January to June 2018) to 4,165 items. Facebook complied with some requests to remove content allegedly violating domestic laws against blasphemy, “anti-judiciary content, and condemnation of the country's independence.”

During the same time period, authorities reported 2,349 profiles to Twitter and...
requested that the platform remove 193 pieces of content. Twitter reported a 0 percent compliance rate with the requests, but did remove content from 204 accounts for violating its terms of service.

In January 2019, Twitter sent a number of journalists, activists, and lawyers notices that published content violated Pakistani law. The notices were allegedly based on “official correspondence,” seemingly from the government or security forces. However, the Information Minister Fawad Chaudhry denied that the government reported the tweets.

The government sent 214 requests to Google to remove 3,125 pieces of content between July and December 2018, up from 196 requests from the previous six months. Of them, 78 percent of requests related to religious offenses, 5 percent to defamation, and 4 percent to hate speech. Google complied with 73 percent of requests. For example, Google removed images and posts that the PTA deemed offensive and blasphemous to Islam and the Prophet Muhammad. In an example with which Google did not comply, the government requested the removal of a YouTube video from Al Jazeera in which Muslim-Americans drew images of their friends named Muhammad.

Social media platforms have also removed content on their own accord. In April 2019, Facebook removed 103 Pakistan-based pages, groups, and accounts from Facebook and Instagram for “inauthentic behaviour” and spamming (see B5). Previously, in August 2018, Twitter removed accounts of Baloch nationalist leaders and political parties, such as the Balochistan Liberation Front (BLF). It was speculated that the accounts were removed in anticipation of twelfth anniversary of Baloch nationalist leader Nawab Akbar Bugti’s death.

Section 38 of PECA limits civil or criminal liability for service providers for content posted by users, unless it is proven that the service provider had “specific actual knowledge and willful intent to proactively and positively participate” in cybercrimes committed under the act.

B3 0-4 pts
Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?

The PTA, the regulatory authority for online censorship, routinely restricts content in a nontransparent and arbitrary fashion. While PECA legally mandates that the PTA issue notices when restricting content, in practice the agency rarely does. This lack
of written notices impedes the ability of those impacted to appeal the orders or undertake judicial review.

PECA, passed in August 2016, gives the government broad blocking powers. Section 37 grants the PTA expansive powers to block or remove any online content that it deems unlawful, “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, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offense under this Act.” Critics contend that such a wide mandate to restrict online speech violates Pakistan’s commitments under the International Covenant on Civil and Political Rights (ICCPR).

Apart from PECA, other regulatory provisions have long enabled politically motivated censorship of dissenting voices and information perceived as damaging to the military or political elites. Broad provisions in the 1996 Pakistan Telecommunications Act support censorship for the protection of national security or religious reasons. A Telecommunications Policy approved in 2015 utilized similar language. Section 9.8.3 enabled the PTA 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.” Section 99 of the penal code separately allows the government to restrict information that might be prejudicial to the national interest.

As a condition of their licenses, ISPs and backbone providers must restrict access to individual URLs or IP addresses upon receipt of a blocking order. Since 2012, successive administrations have sought to move from less sophisticated manual blocking toward technical filtering, despite widespread civil society protests. In 2013, the University of Toronto-based research group Citizen Lab reported that technology developed by the Canadian company Netsweeper, as well as DNS tampering, was filtering political and social content at the national level on the PTCL network.

• **2.** “Pakistan: Telecommunications (Re-organization) Act,” Article 19.
• **4.** PTA Act 1996, article 23.
• **7.** DNS tampering intercepts the user’s request to visit a functioning website and returns an error message.
• **8.** Senft et al., O Pakistan, We Stand on Guard for Thee.
B4 0-4 pts
Do online journalists, commentators, and ordinary users practice self-censorship?

Most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, civil-military relations, separatist movements, and women’s and other minority communities’ rights. A 2017 Digital Rights Foundation report found that women journalists in particular self-censored speech on these issues. In a 2018 survey of Pakistani journalists, 46 percent of those surveyed reported self-censoring due to fears for their safety; 18 percent of respondents reported restricting their reporting to noncontroversial subjects. Self-censorship is also exacerbated by government surveillance and legal repercussions for online speech.

- [2] Ibid.

B5 0-4 pts
Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?

Increasingly, coordinated and inauthentic accounts are manipulating online content and spreading disinformation. Online journalists and activists, especially those scrutinizing the military or intelligence agencies, have also testified to the existence of state-sponsored “troll armies” being employed to silence dissent. For example, in July 2019, following the coverage period, #ArrestAntiPakJournalists trended across Twitter, accompanying tweets containing manipulated information about prominent journalists critical of the ruling party. Many accounts and tweets participating with the hashtag exhibited signs of being automated.

Bots supporting certain political parties also surfaced online ahead of the July 2018 general elections. According to a May 2018 report, 52 percent of accounts
tweeting #PMLN—associated with the popular incumbent Pakistan Muslim League–Nawaz—were bots, while another 46 percent of accounts using #PTI—Imran Khan’s Pakistan Tehreek-e-Insaf—another political party, were as well.\(^\text{4}\)

In April 2019, during the coverage period, Facebook said it had discovered inauthentic behavior on its platform that “was linked to employees of the ISPR (Inter-Service Public Relations) of the Pakistani military.” It removed a number of pages, groups, and accounts that had posted content on or operated pro-military pages, pages related to Kashmir, and more general informational and community pages.\(^\text{5}\)

In July 2018, the government set up a Twitter account to combat fraudulent content,\(^\text{6}\) which has since posted sporadically.\(^\text{7}\)

A report from the Oxford Internet Institute released in September 2019, after the coverage period, identified Pakistan as having coordinated cyber troop teams with full-time staff members employed to manipulate the information space.\(^\text{8}\) The report identifies that such teams work to support preferred messaging of their clients, attack the opposition, and suppress critical content. Pakistan is alleged to have fake accounts run by both bots and human accounts, and most often manipulates content on Facebook, Instagram, and Twitter.

Some individuals have been the targets of apparently coordinated campaigns seeking to discredit them with accusations of blasphemy—a criminal offense which carries a death penalty (see C2). In one example from the previous reporting period, social media users “poisoned” hashtags being used to rally support for missing bloggers, accusing them of blasphemy (see B8).

5. “Removing Coordinated Inauthentic Behavior and Spam from India and
Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

While some digital media outlets struggle to stay financially viable, the online landscape is generally free of major economic or regulatory constraints intended to prevent users from publishing independent political news and opinions.

However, the government has proposed a number of changes to the regulatory system that would give it greater control over digital media and the ability to publish content. For example, legislation proposed in October 2018 would establish the Pakistan Media Regulatory Authority (PMRA)—merging the PTA, Pakistan Electronic Media Regulatory Authority, and the Press Council of Pakistan.1 The PMRA would thus have regulatory control over all electronic, digital, and printed media.2 The proposed legislation would also institute a licensing regime that would restrict online news reporting. According to a concept note circulated by the government, the federal government would have powers to issue directives and the decision of the government will be deemed “final”, ruling out the possibility of judicial review.3 The bill for the PMRA was approved by the federal cabinet in January; there were no further developments on the proposed legislation.4

Separately, the government announced in July, after the coverage period, that it would create media courts that would address media-related disputes.5

2. Steven Butler, “Proposed media regulator provokes strong criticism in
3. Waseem Abbasi, “While regulating media...: Govt decision will be final,” The News International, January 15, 2019,
https://www.thenews.com.pk/print/419168-while-regulating-media-govt-dec...


B7 0-4 pts
Does the online information landscape lack diversity? 24

Despite content restrictions, most Pakistanis have access to international news organizations and other independent media, as well as a range of websites representing political parties, local civil society groups, and international human rights organizations.1

Content online is dominated by users with the greatest access—generally those in urban areas with the means to afford service. While there are several outlets producing content in regional languages, there is a still a disproportionate amount of Urdu and English language content. Further, social taboos and the criminalization of same-sex relationships means that local content addressing the interests of LGBT+ people is limited.


B8 0-6 pts
Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly on political and social issues? 36

Social networking, blogging, and voice-over-IP (VoIP) applications are available and widely used. However, the Securities and Exchange Commission of Pakistan said in March 2017 that “crowd funding is not allowed in Pakistan,” narrowing one potential
avenue for digital activism. The decision was issued in response to activity by a single fraudulent website, but stated that “no company can raise funds” through crowd funding. Further, internet and mobile connectivity are often restricted to limit mobilization and protests (see A3).

The internet has nevertheless provided a space for issues censored on mainstream media. For example, despite facing a complete blackout on print and electronic media, as well as arrests of activists, the PTM has been able to mobilize its rallies across the country. However, engaging in controversial or prohibited activism online has grown increasingly dangerous. Criminal reports filed against activists for their online activity has limited the PTM’s reach.

Online conversations around police brutality and unlawful detentions became more prevalent in Pakistan during the coverage period. There was considerable outrage online about the detentions of academic Ammar Ali Jan, and activist Gulalai Ismail, who were each arrested at separate PTM demonstrations in February. The visibility lent to their detentions online led in part to their speedy releases.

Feminists and women’s rights activists have also used the global #MeToo movement to expose the sexual misconduct of powerful men in Pakistan. However, online accusations have also opened some women up to defamation lawsuits and online attacks (see C7).

6. Rana Bilal, “Meesha Shafi’s lawyers respond to Ali Zafar’s legal notice, ask
C Violations of User Rights

PECA and other laws restrict users’ rights, which were frequently violated during the coverage period. Two users were given the death penalty on charges of posting blasphemous content, although their convictions are under appeal. Government surveillance and social media monitoring were of key concern during the coverage period, as was the continued lack of a data protection law. Users continue to face intimidation, blackmail, and at times violence, in response to online activity.

C1 0-6 pts
Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?

Article 19 of Pakistan’s constitution establishes freedom of speech and freedom of the press as fundamental rights, although they are subject to several broad restrictions, including for “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, commission of or incitement to an offence.” Pakistani courts have not clearly interpreted terms such as “national interest,” “decency,” and “morality,” and parameters of the Article are largely seen as inapplicable to the most powerful institutions in the country.

In a positive development during the coverage period, the Supreme Court reaffirmed the constitutional right to free expression and press freedom in its ruling on the 2017 Faizabad sit-in. Justice Qazi Faez Isa stated in the February 2019 ruling that the government could not restrict the fundamental rights of freedom of speech, expression, and press beyond the limitations defined in Article 19. Although the judgment did not mention these rights in cases of online expression specifically, the sit-in had prompted the blocking of major social media platforms, including Twitter,
Facebook, YouTube, and Instagram.3

Pakistan became a signatory to the ICCPR, which protects freedom of expression, among other fundamental rights, in 2010, but does not consistently uphold it in practice.4 The applicability of international law in local courts is a contentious issue. Pakistan is a dualist country, making international treaties only legally binding once they are specifically incorporated into local law.


C2 0-4 pts
Are there laws that assign criminal penalties or civil liability for online activities?

Several laws restrict the rights of internet users. In August 2016, PECA became law, despite concerns from civil society organizations regarding the lack of transparency involved in the drafting process. Though it contains some procedural safeguards for cybercrime investigations by law enforcement agencies, international and local human rights groups have condemned the law’s overly broad language and disproportionate penalties, including a 14-year prison term for acts of cyberterrorism that the law failed to adequately define.1

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 crimes are punishable with up to seven years in prison. Section 20 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 1 million rupees ($9,500), or both.\textsuperscript{2} The law also grants the PTA broad censorship powers (see B3) and other agencies the ability to conduct wide-ranging surveillance (see C5).

The law’s harsh penalties were cause for particular concern in light of recent sentences passed by antiterrorism courts for online speech. Furthermore, secret military courts were established in 2015 through the 21st amendment to the constitution.\textsuperscript{3} The courts’ jurisdiction lapsed in March 2019 after extensions in 2017; however the government is working to grant another two-year extension.\textsuperscript{4}

IHC has issued directions to add offences of pornography and blasphemy to PECA.\textsuperscript{5} A draft amendment presented to the court in February 2018 included provisions to punish false accusations of blasphemy as well.\textsuperscript{6} In January 2018 the Federal Investigation Agency (FIA) requested that parliament make more offenses cognizable and nonbailable. These included “access, modification, interference, deletion to critical infrastructure, information system or data (sections 6, 7, and 8), electronic forgery (section 13), electronic fraud (section 14), unauthorized issuance of SIM cards (section 17), tampering of electronic equipment (section 18), cyberstalking (section 24), and spoofing (section 26).”\textsuperscript{7} The amendment bill proposed in October 2018 was met with opposition in the assembly, and the bill has been returned to the Senate.\textsuperscript{8}

Sections of the penal code that cover blasphemy—including 295(c), which imposes a mandatory death sentence—are frequently invoked to limit freedom of expression (see C3). In March 2017, the IHC ruled that those accused of posting blasphemous content on social media should be barred from leaving the country until their name is cleared.\textsuperscript{9} Any citizen can file a blasphemy complaint against any other, leaving the accused vulnerable to violent reprisals regardless of whether the complaint has foundation. Human rights groups report that the law lacks safeguards to prevent abuse to settle personal vendettas.\textsuperscript{10}

Other laws threaten online speech. Sections 36 and 37 of the Electronic Transaction Ordinance of 2002 punish “violations of privacy of information” and “damage to information systems,” respectively. The 2002 Defamation Ordinance can impose prison sentences of up to five years. PECA effectively replaced the ordinances, but they were still invoked during the reporting period, and some older cases were also ongoing. Section 124 of the penal code on sedition is broadly worded, and covers acts of sedition “by words” or “visible representation,” which could include digital
speech, though it has not yet been applied to an online context. 11 The Surveying and Mapping Act 2014 limits digital mapping activity to organizations registered with Survey of Pakistan, a government authority, with federal permission required for collaborating with foreign companies. 12

Are individuals penalized for online activities?

People are frequently prosecuted for their online activities, often receiving harsh sentences. The death penalty was imposed in two cases of online blasphemy during this report’s coverage period, although the cases are under appeal.

There have been a number of blasphemy cases against users for allegedly criticizing Islam online. In December 2018, two Christian brothers were sentenced to death for blasphemy for allegedly sharing “disrespectful material” about the prophet Mohammad on their website in 2011. The brothers were originally arrested in 2015. The convictions are being appealed to the Lahore High Court. In addition, death penalty convictions from the previous coverage period are still on appeal. In June 2017, a man was sentenced to death for blasphemy after posting comments about the prophet Mohammad on Facebook. In September 2017, a Christian man was sentenced to death for blasphemy after sending a poem on WhatsApp to a Muslim friend that was critical of Islam.

In another blasphemy case, Patras Masih was arrested in February 2018 for allegedly posting blasphemous content on social media. The arrest came amidst pressure from Tehreek Labaik Ya Rasool Allah and other religious parties. The FIA detained the accused and his cousin, Sajid Masih, and reportedly tortured them (see C7).

Political speech, such as criticism of the government, judiciary, or the armed forces, was subject to legal action during the coverage period. In July 2018, PTM social media activist Hayat Preghal was charged with violating sections 9 and 10 of PECA (for glorification of an offence and cyberterrorism, respectively) and sections 500 and 109 of the Penal Code based on his online comments. He was granted bail three months later, but the charges remain on the books.

In April 2019, journalist Shahzeb Ali Shah Jillani was charged under sections 500 (punishment for defamation), 109 (abatement), and 34 (common intention) of the Pakistan Penal Code read with the Sections 10(a) (cyberterrorism), 11 (hate speech) and 20 (offences against dignity of a natural person) of PECA, for allegedly making defamatory remarks against state institutions. However, in May, 2019 the police’s
first information report that had been filed against the journalist was cancelled as nonmaintainable.10

Does the government place restrictions on anonymous communication or encryption?

Requirements that users link their internet and mobile connections to their national identity card limit anonymous use of the internet. Increasingly stringent security measures mean that users must register 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. Mobile phones must be linked to national identification card number, and unregistered phones have been subject to disconnection.

The government has previously moved to restrict encrypted communication. In 2011, the PTA mandated that ISPs inform them about customers using encrypted tools, including virtual private networks (VPNs). However, the mandate was never properly implemented.


C5 0-6 pts
Does state surveillance of internet activities infringe on users’ right to privacy?

Government surveillance is a serious concern for activists, bloggers, and media representatives, as well as ordinary internet users. PECA grants broad surveillance powers both to agencies within Pakistan and potentially to foreign governments, since it includes provisions that permit the sharing of data with international agencies without adequate oversight.1

In a troubling development during the coverage period, the FIA announced in February 2019 that it would implement a social media monitoring system to target extremism, hate speech, and antinational content online. The system would allow authorities to take action against users under PECA.2 More details have yet to be publicized.

Concerns around social media monitoring spiked in March 2019, after the Interior Ministry ordered an investigation into what it defined as a “targeted social media campaign” against Saudi Arabia while Crown Prince Mohammad bin Salman was visiting Pakistan.3 The ministry’s letter identified journalists and activists who allegedly shared messages “very disrespectful” to the crown prince by including images of murdered journalist Jamal Khashoggi on their social media profiles.
Pakistani law enforcement and intelligence agencies appear to have expanded their monitoring activities, including at the local level, ostensibly to curb terrorism and violent crime. In 2015, the UK-based NGO Privacy International reported that the Pakistani government’s surveillance capabilities, particularly those of the ISI, outstrip domestic and international legal regulation. “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 separate 2013 report by Citizen Lab indicated that Pakistani citizens may be vulnerable to FinFisher spyware, which collects data such as Skype audio, key logs, and screenshots. The analysis found FinFisher’s command and control servers in 36 countries worldwide, including on the PTCL network in Pakistan, but 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.

The Fair Trial Act, passed in 2013, allows security agencies to seek a judicial warrant to monitor private communications “to neutralize and prevent

A Obstacles to Access

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. Warrants can be issued if a law enforcement official has “reason to believe” there is a risk of terrorism; warrants can also be temporarily waived by intelligence agencies. A 2014 white paper issued by the Digital Rights Group said that provisions of the Fair Trial Act contravene the constitution and international treaties that Pakistan has signed.

While there is no data protection law in Pakistan, the Ministry for Information Technology and Telecommunication (MOITT) issued a draft Personal Data Protection Bill during the coverage period. While the bill is a welcome development, it has been criticized for lacking robust safeguards for government-held data.

Data collected by the state’s National Database Registration Authority (NADRA),
which maintains a centralized repository of information about citizens, is not subject to any privacy rules. Data from NADRA and telecom companies, as well as police records, are reportedly sold online, including on Facebook. Given the centralized and interconnected nature of Pakistan’s national database, data is vulnerable when it moves from one department to another.

Pakistanis are also vulnerable to surveillance from overseas intelligence agencies. In June 2015, the online outlet the Intercept published revelations of hacking and infiltration of the PIE by the United Kingdom’s Government Communications Headquarters (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.”

International cooperation on surveillance has also increased since the establishment of the China-Pakistan Economic Corridor (CPEC). Technology such as surveillance cameras and facial-recognition technology has been shared as part of various safe cities initiatives. While these initiatives are framed by the government as measures to protect public safety, the increase in surveillance infrastructure without meaningful safeguards concerns human rights activists.


C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?

Companies are required to aid the government in monitoring users. There is currently no data protection law in Pakistan, despite assurances from the government that it intends to pass one.1 As a result of this lack of oversight, ISPs, mobile companies, and private enterprises are not obliged to maintain or comply with any data protection policies that are in place.2

Under the Fair Trial Act, service providers face a one-year jail term or a fine of up to 10 million rupees ($103,000) for failing to cooperate with warrants (see C5). Section 32 of PECA requires service providers to retain traffic data for a minimum of one year, and allows for that period to be extended with a warrant issued by a court. Furthermore, regulations introduced in March 2018 require all Wi-Fi hotspot service providers to retain user data, including users’ names, national identity or passport number, mobile phone number, time of login and logoff, IP address, MAC address, and internet access log.3

ISPs, telecommunications companies, and SIM card vendors are required to authenticate the Computerized National Identity Card details of prospective customers with NADRA before providing service.4 A reregistration drive was launched following a 2014 terrorist attack on a school that was reportedly facilitated by mobile phones with unregistered SIM cards,5 and the government added a biometric thumb impression to the registration requirements for SIM cards.6 In 2015, those who failed to meet the new requirement were warned of automatic disconnection, and 26 million SIM cards were subsequently blocked.7

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?

Users continue to face intimidation, blackmail, and at times violence, in response to online activism, reporting, and debate, as well as apolitical activity online such as socializing. Users arrested in connection to their online activity are at risk of torture and sexual abuse in Pakistani detention facilities. In past years, online activists have been abducted and held for lengthy periods.

Free expression activists and bloggers have reported receiving death threats online, and Pakistan is one of the world’s most dangerous countries for traditional journalists. 

In June 2018, Daily Times journalist and activist Marvi Sirmed’s house was ransacked and her electronic devices and travel documents were taken. Two days earlier, social media activist and Waqt TV journalist Gul Bukhari was abducted.
by unknown persons, and returned a few hours later.3

In June 2019, after the coverage period ended, blogger and social media activist Muhammad Bilal Khan was killed in a knife attack; he had been active presence on social media, where he promoted causes like interfaith harmony, and called for investigations of enforced disappearances conducted by the military and intelligence agencies.4 Prior to this, in January 2017, five bloggers critical of the establishment, military, or religious militancy, separately went missing from different parts of the country.5 Four of them were recovered around the end of January 2017,6 and the fifth returned home in March 2018.7 The government denied any involvement in the abductions, but one of the recovered activists told the British Broadcasting Corporation (BBC) in March 2017 that he had been held by a “‘government institution’ with links to the military,” and was tortured while he was missing.8

Women are frequently harassed and blackmailed online. Organizers and participants of the 2019 Aurat March, which celebrated International Women’s Day, were subjected to intense online attacks, including death and rape threats.9 In December 2018, an 18-year-old girl in Muzaffarabad died by suicide after a man threatened to upload pictures and videos of her online if she did not meet him.10 In May 2019 it was reported that a girl in Badin died by suicide after being blackmailed over edited pictures.11

Offline sexual violence is often recorded on camera and circulated on social media to both retraumatize and blackmail the survivor. In November 2018, eleven men kidnapped and gang-raped a transgender person in Peshawar. A video of the assault was shared on WhatsApp.12 Another woman was gang-raped and filmed in early 2019.13

Women’s use of digital tools is heavily controlled by families (see A2), and some have been murdered for digital activities in so-called honor killings. In July 2018, a woman in Taxila was killed by her husband for exchanging text messages.14

In one of Pakistan’s most high-profile cases, Qandeel Baloch, a social media celebrity known for openly expressing her sexuality, was killed by her brother in 2016.15 Baloch had sought police protection following threats she received after her real identity was published online.16 Her brother acknowledged killing her because “she was doing videos on Facebook and dishonoring the family name.” The
brother and three other family members were arrested. The trial is ongoing. 17

Separately, in February 2018, Patras Masih and his cousin Sajid Masih were allegedly tortured and ordered to sexually assault each other while in detention for Patras’ social media posts (see C3). To avoid having to carry out the order, Sajid jumped from the fourth floor of the FIA building and was critically injured. 18

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?

Technical attacks against the websites of nongovernmental organizations (NGOs), opposition groups, and activists are common in Pakistan, though many go unreported. During the coverage period 55 female activists and journalists reached out to Pakistan’s Digital Rights Foundation after being targeted by sophisticated email-based phishing attack aimed at obtaining private information.1 During the previous period, Amnesty International reported digital attacks on human rights defenders, such as hacked accounts and devices, and the installation of spyware. The attackers allegedly employed fake online identities and social media profiles to target activists.2 The software used in these attack, Crimson, has
previously been used against Indian military and diplomatic figures.\textsuperscript{3}

There were also reported breaches of data originally collected for government initiatives. Private pictures of citizens from CCTV cameras, collected by the Punjab Safe Cities Authority (PSCA), were leaked, according to January 2019 news reports.\textsuperscript{4} In the absence of a data protection law, those affected have limited opportunities for remedy (see \textsuperscript{C5} and \textsuperscript{C6}). In July 2018, NADRA denied reports of a data breach the previous month, allegedly in which voter demographics were released.\textsuperscript{5}

Cross-border cyberattacks between Pakistan and India continue.\textsuperscript{6} After tensions between the two nations escalated in early 2019 following a deadly suicide attack in Pulwama, a city in Indian-controlled Kashmir, a number of Pakistani sites were allegedly targeted by Indian hackers,\textsuperscript{7} including the website of Ministry of Foreign Affairs.\textsuperscript{8} In the past, hackers on both sides have claimed to target state websites. Among the most serious were reports in 2017 that Indian hackers had targeted Pakistani airports in Islamabad, Peshawar, Multan, and Karachi.\textsuperscript{9}

- \textsuperscript{1} Jahangir, “The mechanics of silencing dissent.”
- \textsuperscript{4} “Safe City Project not so safe as pictures of passengers’ private life leaked,” Pakistan Today, last updated January 20, 2019, \url{https://www.pakistantoday.com.pk/2019/01/20/safe-city-project-not-so-sa...}.
- \textsuperscript{7} “Pulwama attack: Pakistani websites hacked, here's the list,” The Times of India, last updated February 18, 2019, \url{https://timesofindia.indiatimes.com/gadgets-news/pulwama-attack-pakista...}.
- \textsuperscript{9} “India, Pakistan cyber war intensifies,” The News International, January 4,
Explanatory Note

Pakistani-controlled Kashmir is not covered in this report. Certain territories that are assessed separately in Freedom House's *Freedom in the World* report are excluded from the relevant country reports in *Freedom on the Net*, as conditions in such territories differ significantly from those in the rest of the country.

Country Facts

- **Freedom in the World Status**
  - Partly Free
- **Networks Restricted**
  - Yes
- **Social Media Blocked**
  - No
- **Websites Blocked**
Yes

- Pro-government Commentators

  Yes

- Users Arrested

  Yes