PAKISTAN

<table>
<thead>
<tr>
<th></th>
<th>2009</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTERNET FREEDOM STATUS</strong></td>
<td>n/a</td>
<td>Partly Free</td>
</tr>
<tr>
<td>Obstacles to Access</td>
<td>n/a</td>
<td>16</td>
</tr>
<tr>
<td>Limits on Content</td>
<td>n/a</td>
<td>17</td>
</tr>
<tr>
<td>Violations of User Rights</td>
<td>n/a</td>
<td>22</td>
</tr>
<tr>
<td>Total</td>
<td>n/a</td>
<td>55</td>
</tr>
</tbody>
</table>

**POPULATION:** 184.8 million  
**INTERNET PENETRATION:** 11 percent  
**WEB 2.0 APPLICATIONS BLOCKED:** Yes  
**SUBSTANTIAL POLITICAL CENSORSHIP:** Yes  
**BLOGGERS/ONLINE USERS ARRESTED:** No  
**PRESS FREEDOM STATUS:** Not Free

**INTRODUCTION**

With the explosion of mobile-phone use and the gradual spread of broadband internet in Pakistan, access to information and communication technologies (ICTs) has increased, as have citizen journalism and online activism. In response, over the past three to four years—under both military rule and an ostensibly democratic civilian government—the authorities have adopted various measures to exert some control over cyberspace and the sharing of information online. Although the authorities often frame new restrictions as necessary for national security, the war on terror, or protection against blasphemous content, research has revealed that in many cases, hidden under such justifications is an ulterior motive that is political.

In the early 1990s, text-based internet was introduced to the country and the first e-mail service provider in Pakistan, ImranNet,1 was established. The spread of e-mail and digital technologies began to expand with the initiation of the Sustainable Development Networking Programme (SDNP) in December 1992.2 With financial assistance from the United Nations Development Programme (UNDP),3 SDNP succeeded in enhancing computer literacy and providing dial-up internet and e-mail services to urban centers across

---

the country from five nodes based in Islamabad, Karachi, Lahore, Quetta and Peshawar. In 1994-95, Digicom, an entrepreneurial Internet venture, launched the first internet service access point in Karachi. This heralded the beginning of the internet industry in Pakistan. By 2002, the then-Minister of Science and Telecom and his team brought more than 800 cities online across the country via dial-up connections. Internet and mobile-phone penetration spread further with the deregulation of the telecom sector, though a large urban-rural divide persists.

As of 2009, the number of internet users stood at around 20.4 million and there were about one million broadband users as of mid-2010. Mobile-phone penetration is greater. According official figures released in December 2010, there were more than 100 million mobile-phone subscribers with 7 mobile companies, and teledensity including fixed telephone lines, wireless and mobile phones reached 65 percent of the population.

Obstacles to Access

According to International Telecommunications Union (ITU) statistics, the penetration of internet in Pakistan was slightly over 10 percent in 2009. By contrast, the penetration of mobile phones stood at 61.7 percent by the end of 2010. Factors such as poor infrastructure, high costs, low literacy, difficult economic conditions, age, and culture are

---

4 “SDNP Pakistan’s effective use of dial-up UUCP technology to promote communication in absence of connectivity,” Sustainable Networking Development Programme (SDNP), http://www.sdnp.undp.org/countries/as/pk/pkuucp.html.
5 “SDNP Pakistan: Success in Networking for Development.”
some of the constraints that have particularly limited the development and proliferation of the internet in Pakistan. High prices, poor copper wire infrastructure, and inadequate monitoring of service quality by the government regulator have further limited the expansion of broadband internet penetration. Even though the prices for internet use have fallen considerably in the last few years, access remains out of the reach of the majority of people in Pakistan. Most users in Pakistan access the internet either at their workplace or as students at universities and colleges. Cybercafes provide some internet service but are limited to major cities.

In June 2010, the minister in charge of information technologies reported a growth by 150 percent in broadband access since 2008; however, these figures can be misleading given the poor quality of the connections. High quality broadband services remain concentrated in large cities like Karachi, Lahore, and Islamabad. Wireless service providers using WiMAX and EVDO along with mobile operators Mobilink, Ufone, Telenor, Warid, and Zong have also been struggling to attract consumers due to high prices and poor performance and coverage. Pakistan does not yet have a third generation (3G) network, which is also a hindrance for the spread of broadband internet and other wireless services. Remote areas of the country have no access to broadband, and are left with only a slow, intermittent dial-up connection, rendering any meaningful online activities very difficult. This situation is particularly challenging for students in rural areas who seek to study via distance learning, but are then deprived of multimedia lectures and tutorials. In addition, most of the areas in the conflict-stricken Khyber Pakhtunkhwa (formerly Northwest Frontier Province) and the Federally Administered Tribal Areas (FATA) are without internet access at all.

Promoting access to the internet for the masses has not been a development priority for the government, and few resources have been allocated for this purpose. The only example of such an investment has been the establishment of 365 Rabta Ghar (public telecenters in rural areas) by the PTA as a pilot project; however, little information is

---

available on their current status or impact. Financial incentives, cultural traditions, language barriers, and most importantly, the lack of a robust telecommunications infrastructure, also weigh against great expansion of internet connectivity.

In recent years, the Pakistani authorities, either via government order or court decisions, have on several occasions blocked access to various Web 2.0 applications, such as the video-sharing website YouTube, the photo-sharing application Flickr, and the social-networking tool Facebook. Such blocks are often carried out under the rubric of restricting access to “blasphemous” content; however, further research into the individual incidents has found that the restrictions consistently corresponded to circumstances suggesting politically-motivated censorship. The blanket shutdowns have affected a large number of users. For example, the most recent incident was a ban on Facebook that occurred on May 19, 2010 (see details below). At the time, there were approximately 2.5 million Facebook users in Pakistan, and according to Alexa.com, it was the country’s third most popular website.

The first incident of blocking occurred at the end of February 2006 when the Pakistan Telecommunication Authority (PTA) issued instructions to all internet-service providers (ISPs) in Pakistan to block any website displaying the controversial cartoon images of the prophet Muhammad that had been published in a Danish newspaper. The block particularly focused on Google and Blogspot, a blog-hosting service. The ban continued for approximately two months. More recently, upon orders from the Lahore High Court, the PTA, using the pretext of limiting the circulation of blasphemous content, instituted an extensive blockage of internet content from May 19 to 31, 2010. The heightened restrictions were in response to the creation of a “Everybody Draw Mohammed Day” contest on Facebook and a legal appeal initiated by a relatively unknown organization called the Islamic Lawyers Movement. The ban resulted in the blocking of 10,548 websites and critical information sources like YouTube, Flickr, the user-generated online encyclopedia Wikipedia, and more. Mobile-phone providers also halted Blackberry services, at first completely, but then only web-browsing functions. The blocking was widely criticized by

29 Waqar Hussain, “Pakistan Blocks Facebook Over Mohammed Cartoon,” Agence France-Presse (AFP), May 19, 2010, http://www.google.com/hostednews/afp/article/ALeqM5iqKZNldlJFO6c8ctdkUW0C-vkHgEA.
civil society circles, particularly given the collateral damage caused, whereby all users of these particular applications were affected. Responding to public protests, the blanket blocks were generally temporary, and as of the end of 2010, most of these services were available, though the authorities appeared to shift their efforts to blocking individual YouTube videos or Facebook pages instead (see Limits on Content). The exception was access to applications such as Facebook and Twitter via Blackberry devices, which remained restricted throughout 2010, though a range of tips for circumventing the blockage circulated online. ³²

As of December 2010, there were 50 operational ISPs ³³ throughout Pakistan, along with 10 broadband service providers and 2 HFC Operators providing broadband internet. For its backbone, Pakistan is connected via the Pakistan Internet Exchange (PIE) with SEA-ME-WE 3 and 4, along with backup bandwidth provided by Trans-World Associates (TWA). ³⁴ The current total internet bandwidth landing in Pakistan is 105,000 Mbits. ³⁵ The licensing division of the PTA ³⁶ is responsible for licensing telecom service providers including ISPs and mobile-phone providers; cybercafes do not require a license to operate. The process for obtaining a license for an ISP or mobile-phone provider routinely involves long bureaucratic processes and payment of hefty licensing fees. Since there is no regulatory agency to issue licenses, opening a cybercafe is relatively easy. ³⁷

The PTA is the primary regulatory body overseeing internet and mobile-phone services. The Prime Minister appoints the chairman and members of the PTA, and the body reports to the Ministry of Information Technology and Telecommunication. ³⁸ Industry representatives, civil society groups, and independent experts have serious reservations about its openness and independence as a regulatory body.

³³ Internet Service Providers Association of Pakistan (ISPAK) www.ispak.pk.
Since January 2003, the government of Pakistan has taken steps to censor some online content, though the system for doing so is not particularly sophisticated. The authorities primarily rely on a blacklist of URLs that are blocked at both the PIE level and by individual ISPs. According to testing conducted by the Open Net Initiative in 2006 and 2008, censorship efforts focused symbolically on pornography and websites related to religious conversion, with some restrictions being inconsistent across different ISPs. More comprehensively blocked is content perceived as anti-military, blasphemous, or anti-state, while the most systematically censored is information disseminated by Balochi and Sindhi political dissidents. For example, the website of the Washington-based World Sindhi Institute and the website Lal-Masjid are blocked. In November 2010, the authorities blocked The Baloch Hal, the first English language news website focused on Baluchistan, approximately one year after its launch. The authorities have cited Section 99 of the penal code, which allows the government to restrict information that might be prejudicial to the national interest, to justify their blocking.

Despite such limitations, Pakistanis have relatively 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.

However, a confidential document that the PTA submitted to the Lahore High Court in June 2010 and that was later obtained by activists cites a series of policy guidelines that point to government plans to expand content filtering. In this document, the Ministry of IT (MIT) calls for the establishment of a system whereby an opaque Inter-Ministerial Committee for the Evaluation of Websites receives complaints from the public, the ministry, or the PTA, evaluates whether they should be blocked, and if it finds that they should be, issues a directive to the PTA for blocking either the IP address or the URL of the relevant site. The document also includes a list of vaguely worded categories of information.

45 “Country Profile—Pakistan.”
47 Confidential Pakistani document reveals plans for stricter control of the internet and freedom of expression.
considered “unsuitable,” including but not limited to: “information pertaining to any objectionable content,” and websites that “bring contempt to the country or its people,” websites that “undermine Islam or ridicule, disparage, or attack any religion,” websites that bring “contempt of the defense forces, police, air force or any other institution of government,” and websites that contain “propaganda in favor of any foreign state having bearing on any point of disputes or against any friendly foreign state.” If implemented, these policy guidelines would significantly increase restrictions on the free flow of information over the internet.

Indeed, a September 2010 submission by the MIT to the Lahore High Court cited that the committee had begun functioning and was comprised of representatives from the MIT, Ministry of Religious Affairs, Ministry of Interior, security agencies, and the PTA, among others. According to the document, by September 2010, “more than 12,000 blasphemous and anti state/social websites have been blocked from access through the directives of the committee.” Specifically during August-September 2010, over 247 URLs were reportedly blocked, mostly related to an incident of a U.S.-based pastor initiating a campaign to burn copies of the Quran. A list of the banned URLs attached to the submission included web pages from international news outlets like the *New York Times* or the Cable News Network (CNN), blog postings critical of Islam, mostly based in the United States, and dozens of links to YouTube videos or Facebook groups. The submission also referenced growing communication between the Pakistani authorities and administrators for websites such as Facebook and YouTube in order to prompt rapid removal of controversial content, such as the “International burn a Quran day” Facebook group. No further details related to the committee’s scope of work or the criteria used to inform blocking decisions have been made public, however.

Although the professed goal of the government is to limit access to pornographic materials, extremist groups, and anti-state activists, also targeted is certain information perceived as damaging to the image of the military or top politicians. In some incidents, such as the circulation of videos of a member of the armed forces being involved in land grabs, or the President telling members of the audience to shut up in the middle of a public

---

48 Ministry of Information Technology, “Policy Guidelines for Effective Monitoring and Control of Blasphemous/Offensive Content Over Internet in Pakistan.”
51 Ministry of Information and Technology, “Mohammad and Ahmad vs. GOP etc. in the Lahore High Court, Lahore.”
speech, the government has blocked specific URLs; error messages seen by users refer to the censored content as “blasphemous,” or that the “site is restricted,” although it was apparently blocked for political reasons. By contrast, Facebook and Twitter postings by militant Islamic groups such as Hizbut al-Tahrir, including comments inciting violence against the Ahmedi religious minority, have been allowed to circulate with few restrictions.

Most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, or human rights protection for women and homosexuals, given the sensitivity of both the government and non-state actors to these subjects. There were few reports of authorities contacting bloggers to remove specific content or requiring moderators on discussion forums to delete certain messages.

A wide variety of government agencies are involved in online content censorship, but the PTA is the main body overseeing such restrictions. There are no published or known guidelines as to how or why some content is blocked, or what mechanisms may be available for challenging censorship decisions.

The relationship between citizen journalism and traditional media is mutually reinforcing, particularly with respect to a number of daring, investigative bloggers and the circulation of online videos. For example, in August 2010, a YouTube video was posted exposing the brutal killing of two brothers in the presence of senior police officers. Following the video’s circulation, several satellite television stations aired the story as well. This prompted the Supreme Court of Pakistan to initiate a high level inquiry into the killings. In another incident from May 2010, a mobile-phone video showing police humiliating and torturing a woman who approached a police station in Faisalabad to report a theft was posted on YouTube; it too led to departmental inquiries and punishment of the perpetrators. In September 2010, a mobile-phone video appeared online showing Pakistani soldiers arbitrarily killing six civilians as part of an anti-Taliban offensive in Swat valley.

incident drew international attention, including debates within the United States on whether to cut funding to the Pakistani military as a result.  

Although many civil society groups have been able to use the internet to advance their cause, mobile phones are the predominant medium for mobilization around political and social issues. The movement from 2008 to 2010 by lawyers and others calling for the reinstatement of Supreme Court Chief Justice Iftikhar Chaudhry and greater protection of judicial independence is perhaps the most prominent example of how citizens have used social-networking websites, text-messaging, and other new media tools to successfully challenge state repression. The recent floods in Pakistan have prompted many Pakistani citizens and members of the diaspora to mobilize and raise funds online on websites such as Facebook and Twitter.

### ViOlations of User Rights

Article 19 of the Constitution of Islamic Republic of Pakistan grants the fundamental right of freedom of speech, although it is subject to several restrictions. Pakistan also became a signatory to the International Covenant on Civil and Political Rights (ICCPR) in June 2010, although it added several reservations to its instrument of ratification. These reservations include: (a) supremacy of the country’s own constitution; (b) supremacy of Islamic ideology; and (c) self-determination on the provision of rights. In a positive development, in December 2010, a Lahore High Court judge rejected a petition requesting that the Wikileaks website be blocked to protect national security, in the process affirming the public’s right to access such information. The decision raised hopes that it could potentially serve as a precedent for the future protection of citizens’ right to access content online.

---


Several pieces of legislation are used to restrict freedom of expression, including online. In 2008, former president Pervez Musharraf introduced a draconian Prevention of Electronic Crimes Ordinance (PECO). The ordinance called for long prison terms for offenses involving vaguely worded terms like “lewd” and “immoral,” and declared as cyber crimes actions such as sending unsolicited text-messages and circulating photos without the permission of the person who was photographed. The ordinance was widely viewed as an effort to curb the use of digital media in organizing protests or circulating criticism of Musharraf. The regulation lapsed in 2009, but was later tabled before the national assembly for approval to reactivate it. However, in November 2009, the Prime Minister returned it to the National Assembly’s Standing Committee on Information Technology for further consultation and development of a new draft. In doing so, he cited its restrictive approach to free expression as the reason. As of December 2010, the bill was pending and a new draft was still awaited.

Section 124 of the Pakistan Penal Code (PPC) on Sedition is extremely broadly worded, and the 2004 Defamation Act allows for imprisonment of up to five years, though neither is frequently used to punish journalists and has yet to be used to punish online speech. Rather, another section of the penal code, Section 295(c), which addresses blasphemy, was used by police in 2010 to initiate proceedings against Facebook founder Mark Zuckerberg after a user of the social-networking tool created a group hosting a competition to draw the prophet Muhammad, a task considered offensive by many Muslims. The maximum punishment under the law is life imprisonment or the death penalty. Following a wave of jokes about the president that circulated over e-mail, in July 2009 the government announced that several agencies had been tasked with tracing electronically transmitted jokes, and that offenders could face a 14-year prison sentence. Despite such threats and the harsh legal environment, there were no Pakistani bloggers or activists imprisoned for online activities as of the end of 2010.

---

68 “PPC Section 124-Sedition: Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Federal or Provincial Government established by law shall be punished with imprisonment for life to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine.” http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html; Karin Deutsch Karlekar, ed., “Pakistan,” in Freedom of the Press 2010 (New York: Freedom House, 2010), http://www.freedomhouse.org/template.cfm?page=251&year=2010.
Fear of government surveillance is not a significant concern among most bloggers and online activists in Pakistan, with the exception of individuals in Baluchistan. Nevertheless, the Pakistani authorities and particularly intelligence agencies have some monitoring capacity. Before providing services, ISPs, telecom companies, and SIM card vendors are required to verify the National Identity Card details of prospective customers and to authenticate them with the National Database Registration Authority. Although the Electronic Crimes ordinance expired in 2009, ISPs and telecom companies were reported to be continuing to keep logs of customer communications and convey them to security agencies as needed under directives from the PTA. In recent years, provincial authorities have pressured the central government to grant greater surveillance powers and location tracking ability to local police as part of efforts to curb terrorism and violent crime. As of the end of 2010, it was unclear how much the authority had been broadened. According to some reports, the PIE positioned at the international internet gateway has the capability to monitor all incoming and outgoing traffic, as well as store all e-mails. In addition, Pakistan is reported to be a customer of Narus, a U.S.-based firm known for designing technology that allows for monitoring of traffic flows, as well as deep-packet inspection of internet communications.

Although Pakistan is one of the most dangerous environments for traditional journalists, with at least 12 being murdered in 2009 and 2010, no bloggers or online activists have been killed to date. However, during the internet crackdown that occurred in May 2010, there were several incidents of non-state actors, particularly Islamic extremists, attacking or threatening bloggers and others who were advocating against the blocking of online resources. In one instance, a mob attacked a press conference organized at the Karachi Press Club, though the club’s personnel were able to disperse the tensions. During

---


the same period, several free expression activists and bloggers received anonymous death threats. Most such messages were sent via text message from untraceable, unregistered mobile-phone connections, usually originating from the tribal areas of the country, and several had very specific details related to the individuals’ profile or recent activities. Similarly, as some militant Islamic groups consider cybercafes to be sites of moral degradation, they have initiated attacks and bombings of such access points. Most attacks have occurred in Khyber Pakhtunkhwa Province and FATA, but in July 2010, bomb blasts also struck two cybercafes in Lahore, injuring six people.77