Bangladesh

PARTLY FREE

44/100

A. Obstacles to Access 13/25
B. Limits on Content 17/35
C. Violations of User Rights 14/40

LAST YEAR’S SCORE & STATUS
49/100 Partly Free

Scores are based on a scale of 0 (least free) to 100 (most free)
Overview

Constraints on internet freedom in Bangladesh tightened during the coverage period. The government used a variety of methods to restrict the online space; authorities blocked critical websites, circumscribed mobile networks to limit communication and mobilization, announced new surveillance programs, and arrested journalists and users alike. Pressure on online journalists and activists peaked around mass protests calling for improved road safety and other reforms, as well as the 2018 general elections, which were marred by election irregularities and violence. Even after the elections, in 2019, authorities blocked a number of critical news sites, revealing its continued desire to suppress dissenting voices.

The ruling Awami League (AL) has consolidated political power through sustained harassment of the opposition and those perceived to be allied with it, as well as of critical media and voices in civil society. Corruption is a serious problem, and anticorruption efforts have been weakened by politicized enforcement. Due process guarantees are poorly upheld and security forces carry out a range of human rights abuses with near impunity.

Key Developments, June 1, 2018 – May 31, 2019

• Mobile service was frequently restricted around the December 2018 general elections. Skype was also temporarily blocked to thwart communication between exiled opposition leaders and local activists (see A3).
• During demonstrations for improved road safety and other reforms in August 2018 that were marred by violence, the Bangladesh Telecommunication Regulatory Commission (BTRC) throttled 4G and 3G service to limit protesters’ ability to live stream and share video content (see A3 and B8).
• Authorities stepped up their blocking of websites that oppose the government or publish critical reports during the coverage period, including sites ahead of
the election and multiple news sources in 2019 (see B1).

- In September 2018, the Digital Security Act (DSA) went into effect, which imposes harsh prison sentences for online defamation, insulting a person’s religion, and a number of other offenses that could be used to stifle online dissent (see C2).
- A surge of arrests under a range of laws, including the new DSA, further threatened online expression. One user was convicted to seven years in prison in January 2019 for sharing photoshopped images of the prime minister and other politicians (see C3).
- In October 2018, the government allocated 1.2 billion takas ($14 million) to a new social media monitoring program to identify “fake news” and propaganda online (see C5).

A. Obstacles to Access

_The number of internet users in Bangladesh is steadily increasing. More than 90 percent of users access the internet via mobile service providers, which recently began offering faster 4G service. Users continue to complain about the high cost of private internet service. Restrictions on connectivity to mobile internet service and social media platforms increased in the coverage period, notably during key political events._

A1 0-6 pts

| Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections? | 3/6 |

Information and communications technology (ICT) usage is rapidly increasing in Bangladesh, although it lags behind many other countries around the world. According to recent publicly available data from the International Telecommunication Union (ITU), internet penetration in Bangladesh was 15 percent at the end of 2017. Government estimates of internet penetration were significantly higher in March 2019, at 55 percent. In 2019, approximately 93 percent of users accessed the internet via mobile service providers, which only recently began offering faster 4G
service. 3 The remainder obtain service through a traditional internet service provider (ISP) (around 6 percent) or one of the three wireless WiMax operators (less than 1 percent). 4 According to the Alliance for Affordable Internet, only 23 percent of the population had access to mobile broadband services in 2018.

The Economist Intelligence Unit’s Inclusive Internet Index 2019 report ranks Bangladesh 69 out of 100 countries in terms of availability, determined by “quality and breadth of available infrastructure.” 5

A2 0-3 pts

| Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons? | 1/3 |

Internet access is prohibitively expensive for many lower-income individuals, and access is limited in rural areas. According to the Inclusive Internet Index 2019 report, Bangladesh ranks 70 out of 100 countries surveyed for affordability, defined by cost of access relative to income and the level of competition in the internet marketplace. 6

Access to the internet varies depending on socioeconomic status and geography. In recent years, the government has reduced the bandwidth price to access the internet significantly. However, according to some users, reductions in bandwidth at the wholesale level have not led to lower prices for many individual customers. 7 Users complain about the high cost and lower quality of internet service in rural areas.

The government has taken some action to address the disparity in internet access among certain segments of society. For example, the government’s Digital Bangladesh by 2021 program, established in 2009, seeks to integrate efforts to improve internet access with development programs in national priority areas, such as education, healthcare, and agriculture. 8 By the end of 2018, more than 4,554 Union Digital Centers had been established, with the goal of providing low-cost internet access and related e-services among low-income and other underserved communities, such as rural women and people with disabilities. 9
In 2017, citing security concerns, the government banned telecommunications providers from selling mobile phone connections to Rohingya refugees, undermining access to the internet for hundreds of thousands of people who had fled to Bangladesh from neighboring Myanmar. The government also threatened providers with fines if they ignored the ban. ¹⁰ However, the ban was not widely enforced and many Rohingya maintained mobile phone access. In September 2019, however, after the coverage period, the government again ordered mobile service providers to cease selling SIM cards to Rohingya refugees and said it would deactivate any of their existing SIM cards. ¹¹

A3 0-6 pts

**Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?**

Authorities increased their restrictions on the internet and communication services during the coverage period. While the government tested an internet shutdown in early 2018, a number of shutdowns targeted connectivity during the elections and mass protests, representing a clear escalation by the government. Skype was also briefly blocked in the run-up to the December 2018 elections.

The BTRC throttled mobile service around the general elections in December 2018, which were marred by violence. Both 3G and 4G service was unavailable several times in the run-up to the election, and again on election day. ¹²

Internet access was also restricted during other tense political moments. In August 2018, amid popular student protests for safer roads and other reforms, which also led to police violence, the BTRC ordered ISPs to restrict 3G and 4G services for 24 hours, only allowing 2G mobile service (see B8). ¹³

After the coverage period, in September 2019, authorities reportedly restricted 3G and 4G mobile service in Rohingya refugee camps, escalating an existing crackdown on connectivity for the vulnerable Rohingya refugee community (see A2). ¹⁴
In early 2018, the BTRC announced plans to suspend internet service nationwide during designated time periods in February, in order to prevent questions for the national secondary school exams from leaking online. 15 On February 11, 2018, the BTRC conducted a test run, in which internet service was shut down for 30 minutes. The following morning, internet service across the country was suspended as part of the official policy. However, the unpopular policy was reversed after just 10 minutes in the wake of a public backlash. The BTRC restored internet service within 20 minutes of its decision to reverse the policy 16

The government occasionally restricts access to social media and communications platforms. Before the national elections, the BTRC briefly blocked Skype in November 2018 to thwart communication between exiled leaders of the opposition and their activists on the ground. 17

The government manages the fiber-optic infrastructure connecting Bangladesh with international undersea cables. However, the majority of the gateways and internet exchange points (IXPs) are privately owned and managed.

Bangladesh’s physical internet infrastructure was historically vulnerable, relying on the undersea cable SEA-ME-WE-4, which connects Southeast Asia, the Middle East, and Western Europe. 18 Since late 2012, however, Bangladesh is also connected via an international terrestrial cable managed by private companies, reducing the risk of service being completely lost in the event of problems with the undersea cable. 19

A4 0-6 pts
Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers? 5/6

There are no serious legal, regulatory, or economic obstacles that restrict the diversity of service providers. As of June 2019, 129 ISPs operated nationwide, with no clear market leaders. 20

http://www.btrc.gov.bd/sites/default/files/operator_list/ISP_Nationwide....
Users only have four options for mobile connections. At the end of March 2019, Grameen Phone, owned by Telenor, had the largest market share at 46 percent, followed by Robi with 29 percent, and Banglalink with 21 percent. The state-owned Teletalk holds the remaining share of the market.

**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?

1/4

Officially, the BTRC is an independent regulatory body responsible for overseeing telecommunications and related ICT issues. However, in practice the body lacks independence and represents the interests and priorities of the government.

The BTRC was established under the Bangladesh Telecommunications Act of 2001. The government amended the act in 2010, making the Ministry of Post and Telecommunications responsible for regulation of the telecommunications sector, with the BTRC acting as an auxiliary organization. This move led to a number of administrative delays, including for the announcements of new tariffs and license renewals. In 2014, the Ministry of ICT merged with the Ministry of Posts and Telecommunications. In addition, the prime minister’s office has an access to information program supported by the UN Development Program, which has considerable influence over top-level ICT-related decision-making.

**B. Limits on Content**

Authorities imposed significant restrictions on content during the reporting period. Mobile networks were restricted to limit mass protests, while a range of websites and news sites critical of the government were blocked. In the run-up to the elections, both Facebook and Twitter removed accounts allegedly linked to state-sponsored actors that were spreading disinformation.

**B1** 0-6 pts

Does the state block or filter, or compel service providers to block or filter,
During the coverage period, authorities blocked a host of websites critical of the government. 26 The government also carried out a campaign to block pornographic and gambling sites, which led to the blocking of platforms such as TikTok and a popular blogging site.

In December 2018, the BTRC blocked 58 news websites for “national security” reasons and for publishing “fake news” ahead of the general elections. 27 Some of the blocked websites supported opposition parties. 28 Four of the sites were unblocked after one day—priyo.com, Poriborton, dhakatimes24.com, and risingbd.com. 29 The 54 other sites remained unavailable at the end of the coverage period. 30

Access was restricted to a range of other news outlets outside of the election period. In April and May 2019, Bangla.report and Poriborton, two popular news sites, were blocked. 31 While no official explanations were provided for the blocks, some analysts suspect that they were targeted for publishing articles critical of the government. As of July 2019, Bangla.report was accessible within Bangladesh, while Poriborton remained blocked.

In March 2019, both Al Jazeera’s English website and the local news and discussion site Joban were temporarily blocked after publishing reports accusing the country’s top security adviser of using military intelligence officials to abduct three men involved in a business dispute with the official’s wife. 32 The government denied responsibility for the blocking. 33

In June 2018, journalists at the Daily Star—a leading English-language daily newspaper in Bangladesh—reported that the BTRC ordered its website blocked after the outlet published a report on the alleged murder of Teknaf municipal councillor Akramul Haque. The site was down for at least 18 hours before access was restored. 34

The government ramped up its efforts to block pornography and gambling sites following a November 2018 High Court ruling (see B3). Beginning in February 2019, the BTRC blocked more than 20,000 pornographic and gambling websites. 35 The
social media apps TikTok and Bigo Live were also blocked for containing pornographic content. The largest Bengali blogging website, with approximately 250,000 registered users, was also reportedly blocked.

Social media and communication apps have occasionally been subject to blocking. Before the national elections, the BTRC briefly blocked Skype (see A3). In August 2018, the government also threatened to block Facebook and to introduce content filtering for social media usage in the country. Previously, Facebook reported “a disruption affecting access to Facebook products in Bangladesh” in 2016, which was possibly related to a network shutdown test. In 2015, Facebook, Facebook Messenger, WhatsApp, and Viber were among several platforms temporarily blocked. Similarly, the communications apps Threema and Wickr were blocked from May 2016 into mid-2018.

Authorities employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete legitimate content. Many cases are not publicly disclosed.

Authorities have threatened websites with legal action or blocking if critical content is not removed. The editor of the news outlet Bangla.report alleged that the minister of posts and telecommunication threatened to take legal action if the website did not remove an article about an individual who wanted to meet with the minister at a business summit. After declining to remove the content, the website was temporarily blocked (see B1).

The government periodically asks private companies to remove content. Google reported that officials made eight removal requests affecting 74 pieces of content for defamation, fraud, criticism of the government, and violence between January and June 2018. From January to December 2018, Facebook removed one video for alleged impersonation.
Progovernment actors also employ informal means of removing online content. Journalists critical of the government have had their Facebook accounts restricted. Some analysts suspect these restrictions were carried out as a result of progovernment actors misusing Facebook’s mechanism to report content that violates the platform’s community standards. 44

B3  0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?  
1/4

The process for restricting internet content lacks transparency, and there is no independent appeals process in place for blocked websites or content removal orders. Further, the government’s increasing restrictions on connectivity and social media platforms are disproportionate and lack transparency.

The BTRC censors content primarily by issuing informal orders to domestic service providers, which are legally bound by their license and operations agreements to cooperate. Service providers have described official censorship as ad hoc in nature, without follow-up mechanisms in place to ensure compliance. 45 For example, no official notice or explanation was given to ISPs before or after they were compelled to block Poriborton and Bangla.report (see B1). No appeals have been documented in response to censorship directives.

Courts have also ordered restrictions on internet content. In November 2018, for example, the High Court requested that authorities block all pornography websites and obscene material for six months (see B1). 46 The court also ordered the government to explain whether all pornographic websites should be made illegal.

B4  0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?  
1/4
Online journalists and social media commentators continue to report a climate of self-censorship on political and religious topics in Bangladesh. A series of fatal attacks on bloggers in recent years (see C7), coupled with an increase in criminal charges against online journalists and other internet users under the ICT Act and the newly enacted DSA (see C3), have exacerbated online self-censorship. In a report published by Human Rights Watch in December 2018, one journalist reported publishing only 10 to 20 percent of the news available, while another reporter claimed to self-censor 50 percent of the time. 47

 Authorities do not officially pressure or coerce news outlets, journalists, or bloggers to follow a particular editorial direction in their reporting. However, disinformation that circulated on social media was linked to the government during the coverage period.

 Ahead of the elections in December 2018, Facebook reported removing coordinated inauthentic behavior that was linked to the government. 48 The pages removed purported to be independent news outlets, yet disseminated antiopposition and progovernment content. Also in December 2018, Twitter removed a “very small” number of accounts, some of which are apparently connected to state-sponsored actors, that were engaged in “coordinated platform manipulation.” 49

 During a campaign rally in September 2018, a senior government advisor encouraged the political activists in the ruling party to be more active online by flooding social media with new accounts, using both real and fake names. 50 The government has allegedly started new online monitoring efforts to stop the spread of disinformation following the student protests (see C5). 51 Similarly, in January 2019, the newly appointed information minister promised to crack down on “fake news.” 52
Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?  

During the coverage period, there were no documented economic constraints imposed on online media outlets or other users by the government. However, some regulatory constraints affect the ability of online outlets to publish. In 2015, the government imposed mandatory registration requirements on news sites and daily newspapers that publish online, and authorities threatened to cancel the accreditation of journalists working for unregistered media outlets. 53 The government justified registration as a tool to constrain the purported abuse of media to destabilize society. 54 However, no penalties have been reported for noncompliance.

B7 0-4 pts

Does the online information landscape lack diversity?  

The online media landscape in Bangladesh is vibrant, with a number of online outlets that give voice to a range of views. Even with the increased level of censorship during the coverage period, people are able to access a variety of local and international news sources that convey independent, balanced views in the main languages spoken in the country. The ability to access localized information and create content in Bengali has contributed to the popularity of local blog hosting services. 55 Online media outlets, social media platforms, blogs, and websites represent diverse interests within society. While Bangladesh’s minority ethnic groups are inadequately represented in the mainstream media, the popularity of social media and news sites have brought new voices to the fore. However, the blocking of social media platforms and communications apps has at times threatened the diversity of online content (see B1), though many people use virtual private networks (VPNs) to bypass blocking. 56

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

While social media platforms, communications apps, and other digital tools remain largely accessible to users who wish to mobilize and campaign, the government restricted 4G and 3G service in an effort to limit mass protests in Dhaka and other parts of the country in August 2018. The throttling reduced protesters’ ability to live stream and share other video content amid reports of violence during the demonstrations. 57

Social media platforms, particularly Facebook, played a significant role in the August protests calling for better road safety, as well as April 2018 demonstrations against a quota system used to fill certain public service positions. Protesters used Facebook to mobilize, and both protesters and the government employed the platform to advocate their positions. During the road safety protests, photos and videos were shared using the hashtags #WeWantJustice, #RoadSafetyMovement, and #bengladeshstudentprotests. 58 In a troubling move, however, the Dhaka police invoked cybercrime laws to open investigations against demonstrators for allegedly spreading propaganda online (see C3). 59 The government implemented a similar heavy-handed approach against political opponents during the run-up to the national elections in December 2018 (see C3 and C7).

C. Violations of User Rights

Violations of user rights intensified during the coverage period, with violence against online activists and journalists, as well as a surge of arrests around both the general elections and student protests. Within this more repressive environment, authorities also ramped up their efforts to monitor social media through sophisticated surveillance technology. Meanwhile, the 2018 DSA went into effect, which has more restrictive provisions than its predecessor, the IT Act.

<table>
<thead>
<tr>
<th>C1</th>
<th>0-6 pts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do the constitution or other laws fail to protect rights such as freedom of</td>
<td></td>
</tr>
</tbody>
</table>
While online expression is recognized in the constitution, it remains largely unprotected in practice. Article 39 (1, 2) in Chapter 2 of the constitution recognizes the freedoms of thought, conscience, and speech as fundamental rights, and online expression has historically been considered within the scope of this provision. However, other laws undermine these rights and internet users frequently face criminal penalties for free expression protected under international human rights standards.

The 2006 ICT Act defines and ostensibly protects freedom of expression online, though it also includes an array of penalties for citizens who violate others’ rights to communicate electronically (see C2). The DSA, which was passed by the parliament in September 2018, is ostensibly meant to prevent cybercrime and will replace parts of 2006 ICT Act, but contains provisions that can infringe on free expression online (see C2).

Sections 68 and 82 of the ICT Act, which were not annulled by the DSA, contain provisions for a Cyber Tribunal and Cyber Appellate Tribunal to expedite cybercrime cases. In 2018, there was one Cyber Tribunal in Dhaka, headed by a low-ranking member of the judiciary. The Appellate Tribunal, which can reverse the Cyber Tribunal’s rulings, is yet to be formed.

The judicial system of Bangladesh is formally independent from the executive and legislative branches, but critics assert that it can be partisan. Police and regulators generally bypass the courts to implement censorship and surveillance without oversight.


C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online
Online activists, journalists, and other users regularly face civil and criminal penalties for online expression. Notably, Section 57 of the 2006 ICT Act outlines prohibitions on the electronic dissemination of defamatory, obscene, or false information, with violations punishable by a minimum of seven years imprisonment and fines of up to 10 million takas ($125,000). In 2013, the ICT Act was amended, increasing the maximum prison term for those convicted from 10 to 14 years.

In September 2018, the parliament approved the draft DSA; the cabinet first approved the act in early 2018. While Section 57 of the ICT Act was repealed by the legislation, the new law imposes similarly restrictive provisions. Section 21 provides for sentences of up to 14 years in prison for anyone who uses digital devices to spread negative propaganda regarding the Liberation War or the father of the nation. Section 25 introduces sentences of up to three years in prison for deliberately publishing intimidating or distorted information against an individual online. Section 28 mandates up to 10 years in prison for harming someone’s religious sentiments. Section 29 provides for up to three years in prison for publishing information intended to defame someone. Section 31 provides for sentences of up to seven years in prison for deliberately publishing information that can spread hatred among communities. Section 32 has been criticized by rights groups for potentially stifling investigative journalism by imposing sentences of up to 14 years for recording or accessing information digitally without prior consent.

Under the DSA, no warrant is required before making ICT-related arrests, and some crimes are “nonbailable,” meaning suspects must apply for bail at a court.
In Bangladesh, individuals are frequently penalized for online activities that are protected under international human rights standards. The number of arrests and prosecutions under the ICT Act and the newly introduced DSA increased during the coverage period.

In January 2019, Monir Hossain was sentenced to seven years in prison and fined 10,000 takas ($118) after being convicted under Section 57 of the ICT Act, despite its recent repeal, for sharing photoshopped images of the prime minister and other politicians using his mobile phone. He was originally charged in 2013. 67

Between July and September 2018, a crackdown on the road safety and job quota protest movements led to approximately 100 arrests and 52 cases filed under Section 57 of the ICT Act, sections of the penal code, and the Special Powers Act (see B8). 68 Authorities used social media content—including likes, shares, and posts—as justification for many of the arrests. 69 Most were charged with spreading false information or working to destabilize the country. The internationally renowned photojournalist Shahidul Alam, a school teacher, an academic at Chittagong University, and a popular actress were also arrested for online posts in connection with the protest movements under Section 57, 70 while a prominent online activist went into hiding for fear of arrest. 71 Alam was later granted bail after spending over 100 days in prison, where he was allegedly beaten (see C7). The academic was granted bail after 37 days in prison. 72 Furthermore, the cyber unit of the Dhaka Metropolitan Police identified and charged 28 social media account owners they alleged to be spreading “fabricated and misleading” information that instigated students during the protests. 73

A number of journalists, activists, and opposition figures have been arrested under the DSA, including those reporting on election irregularities. 74 In January 2019, Abu Raihan Al-biruni, an editor and staff reporter for the news site Banglamail24, was arrested for spreading false information and rumors about top government officials and political figures online. 75 In December 2018, Sheikh Riad Muhammad Noor, acting editor for the news site daily71.com, was arrested and charged with posting seditious, false, and baseless news on social media. 76 Additionally, on February 2019, prominent newspaper journalist Abu Zafar was arrested under DSA for reporting
against the corruption of a senior police officer. 77 Four other journalists from the outlet were sued under DSA. 78

The government has also targeted expatriate Bangladeshis for criticizing the government online. According to a senior officer of the Criminal Investigation Department (CID) of the Bangladesh Police, cases were filed against at least 12 expatriates in the United Kingdom, Malaysia, Saudi Arabia, Qatar, Australia, and Oman for allegedly spreading antistate rumors on social media. 79

**C4** 0-4 pts

| Does the government place restrictions on anonymous communication or encryption? | 2/4 |

The government does not impose registration requirements on bloggers or internet users, registration is mandatory for online news portals (see B6). However, biometric registration in the form of fingerprints, national identity cards, and related personal information, are required to obtain a mobile connection, curtailing anonymous communication. 80

Bangladeshi users are not prohibited from using encryption services to protect their communications. There are no laws requiring users or providers of encryption services to turn over decryption keys to the government.

**C5** 0-6 pts

| Does state surveillance of internet activities infringe on users’ right to privacy? | 2/6 |

Bangladesh recognizes the right to privacy and correspondence under Article 43 of the constitution. 81 However, there is no specific privacy or data protection law, leaving internet and mobile phone users vulnerable to surveillance or other violations of their privacy. 82
There were a number of worrisome privacy and intrusive surveillance developments over the coverage period. In October, the government announced a new social media monitoring program to identify “fake news” and propaganda online. The project reportedly began in November and is overseen by the Rapid Action Battalion (RAB), a special forces unit that has been implicated in human rights abuses.  

The program’s initial budget was 1.2 billion takas ($14 million). Similarly, in August, authorities announced that the police would establish a cybercrime monitoring cell in each local district across the country to monitor “cybercrime” and the spread of rumors, including on social media. It is unclear whether this program is connected with the RAB’s monitoring efforts.

The privacy rights of mobile phone users have also been threatened. In December 2018, it was revealed that the BTRC had collected the personal information of about 70 million mobile subscribers and shared it with other government agencies for a purported “survey.”

In 2017, news reports revealed that the government was planning to install internet monitoring equipment worth approximately $19 million by May 2018, under a project titled “Cyber Threat Detection and Response.” The equipment would perform granular analysis of network traffic using deep packet inspection (DPI) in order to help the government enforce the ban on pornography and conduct monitoring to combat militancy, the reports said. There were no new developments during the coverage period.

The Home Ministry submitted a proposal in 2015 to purchase approximately $25 million worth of equipment from foreign companies to upgrade its mobile telephony, internet, and related surveillance networks. The proposal requested that a cabinet committee on economic affairs relax procurement regulations to facilitate the purchase, which would enable the National Telecommunication Monitoring Center (NTMC) to conduct “lawful interception” to assist local law enforcement agencies. The center has operated under the Home Ministry since 2014, according to news reports. Foreign companies listed in the proposal include the US firms Verint Systems and SS8, German firms Trovicor and UTIMACO, the Italian firm RCS, the Chinese firm Inovatio, and the Swiss firm New Saft. The companies advertise equipment
capable of analyzing data traffic, calls, emails, and audiovisual materials online. The status of the proposal as of the end of the coverage period was unclear.

In 2014, the UK-based nonprofit Privacy International reported that the RAB sought to purchase mobile surveillance technology from a company based in Switzerland. The technology would allow police to “indiscriminately gather data from thousands of mobile phones in a specific area and at public events such as political demonstrations,” according to the group.89 The same year, leaked documents about a Bangladesh law enforcement agency’s 2012 purchase of FinFisher software distributed by Gamma International, which is used to monitor digital traffic, was published on WikiLeaks.90

<table>
<thead>
<tr>
<th>C6</th>
<th>0-6 pts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are service providers and other technology companies required to aid the government in monitoring the communications of their users?</td>
<td>2/6</td>
</tr>
</tbody>
</table>

Service providers and technology companies are required to aid the government in monitoring the communications of their users. Rights groups have raised concerns about the security of the country’s mobile phone registration process and possible access to biometric data by third parties (see C4).91

http://www.daily-sun.com/printversion/details/119870/Biometric-SIM-Regi...-

The government can request that telecommunications providers retain the data of any user for an unspecified period, according to the 2001 Bangladesh Telecommunication Regulatory Act.92 The act was amended in 2010, and now allows the government to intercept electronic voice or data communications from any individual or institution without a court order to ensure the security of the state. The act also requires domestic service providers to cooperate with the government in intercepting such communications, though there are no clear provisions governing the process or the penalties for noncompliance.93

In 2017, Facebook refused to sign a memorandum of understanding with the Bangladesh police, which had requested that Facebook require additional
identification, including national ID numbers, from Bangladeshi nationals to register with the social network. 94

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? 2/5

During the coverage period, online journalists and ordinary users faced violence, including during student protests and the national elections.

Amid the student protests, journalists and ordinary users were subjected to violence. While renowned photojournalist and online activist Shahidul Alam covered the protests and shared updates via social media in August 2018, government supporters attacked him and reportedly broke his camera. 95 Alam was later arrested and allegedly beaten while in detention (see C3). Journalists reporting on the elections and allegations of fraud were also subjected to violence, and some alleged that they were forced to delete photos of their reporting. 96 Al Amin, a reporter for the news site Cvoice24.com, was beaten by 15 men as he tried to enter a polling station on election day. 97

Journalists and others who speak out on controversial issues have been killed in the past, although no such deaths were linked to online activity during the coverage period. 98 A series of bloggers murdered from 2013 to 2016 has had a deleterious affect on internet freedom. Although local Al-Qaeda branches claimed responsibility in some cases, 99 police have said that local radical groups, notably the Ansarullah Bangla Team, recruited and trained students and religious teachers to execute the targets, frequently using machetes. 100 Many bloggers left the country or sought asylum abroad. 101 Others expressed their determination to continue writing. 102 Little progress has been made in the investigations of the bloggers murdered.

C8  0-3 pts

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

No cyberattacks on news sites and blogs were documented in Bangladesh during the coverage period. Private sector actors are frequently subjected to technical attacks. In May 2019, three Bangladeshi banks were victimized by cyberattacks. One of the banks, Dutch Bangla Bank Limited (DBBL), lost approximately $3 million in the attack. 103 The DBBL attack was one of the most prominent cyberattacks since the 2016 hacking of a computer at the Central Bank, in which millions of dollars were transferred to a bank in the Philippines, highlighting wider cybersecurity vulnerabilities. 104 ISPs have informally organized a cyber emergency response team to address online threats. 105

Footnotes

2  Calculated based on number of internet subscribers reported by the Bangladesh Telecommunication Regulatory Commission as of March 2019 and Bangladesh’s population during the same period, http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-march-20...; https://www.worldometers.info/world-population/bangladesh-population/
3  http://www.thedailystar.net/frontpage/bangladesh-enters-4g-internet-ser...;
5  “Inclusive Internet Index,” Economist Intelligence Unit, https://theinclusiveinternet.eiu.com/explore/countries/BD/?category=ava....

More footnotes
On Bangladesh
See all data, scores & information on this country or territory.
See More ▸

**Country Facts**

Global Freedom Score

39/100  Partly Free

Internet Freedom Score

42/100  Partly Free

Freedom in the World Status

Partly Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

No

Users Arrested

Yes

**In Other Reports**

Freedom in the World 2019

**Other Years**

2020
Be the first to know what’s happening.

Join the Freedom House monthly newsletter

Email

Subscribe

ADDRESS
1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org

@2020 FreedomHouse