Bahrain

Not Free
29
100

A Obstacles to Access    16 25
B Limits on Content      8 35
C Violations of User Rights 5 40

Last Year's Score & Status
29 100 Not Free

Overview
Internet freedom in Bahrain remains restricted. While no internet shutdowns were reported during the coverage period, numerous websites continued to be blocked, social media users were arrested and jailed, and the level of self-censorship and state surveillance remained high. Journalists and activists who work online, including those abroad, continued to face extralegal intimidation, and reports continue of their severe abuse while in custody of Bahraini authorities. The government works to manipulate and control online information.

Bahrain was once viewed as a promising model for political reform and democratic transition, but it has become one of the Middle East’s most repressive states. Since violently crushing a popular prodemocracy protest movement in 2011, the Sunni-led monarchy has systematically eliminated a broad range of political rights and civil liberties, dismantled the political opposition, and cracked down harshly on persistent dissent in the Shiite population.

**Key Developments**

**June 1, 2018 – May 31, 2019**

- In contrast to past years, no restrictions to connectivity were observed during the reporting period (see A3).

- In April 2019, authorities announced progress on plans to establish a single national broadband network, which is expected to be completed later in 2019 (see A4).

- Video recordings and live-streamed video of government proceedings were censored or removed on several occasions, apparently to prevent users from viewing potentially controversial or embarrassing remarks by officials (see B2).

- In May 2019, the cybercrime directorate of the Ministry of Interior (MOI) declared the accounts of several Bahraini activists and journalists to be malicious, and a few days later sent SMS messages and tweeted to users to warn them that following “malicious” social media accounts could result in
prosecution (see B5, C7).

- Between June 2018 and May 2019, at least 21 individuals were arrested, detained, or prosecuted for their online activities, with some still on trial as of May 2019. In December 2018, Nabeel Rajab, one of Bahrain’s most prominent human rights defenders, lost a final appeal of a five-year sentence handed down by the Supreme Court months earlier on charges that included “spreading false news during a time of war,” “insulting a neighboring country,” and “insulting a statutory body” (see C3).

- Unregistered SIM cards were disconnected as government regulations went into effect (see C4).

- In October 2018, a month before parliamentary elections, the MOI announced that it was monitoring phone messages and would take action against those involved in illegal activities (see C5).

- Journalists and activists in Bahrain continued to face extralegal intimidation and abuse in custody. Activists and other users continued to flee Bahrain due to threats to their safety. Bahraini activists abroad faced threats and intimidation (see C7).

**A Obstacles to Access**

*Bahrain is one of the most connected countries in the world. Competitive prices for broadband data services have led to high levels of mobile internet penetration. Internet shutdowns were not reported during the coverage period. The government announced progress in its plan to establish a single national broadband network.*

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

There are no infrastructural limitations to the internet in Bahrain, where internet
penetration stood at 98.6 percent at the end of 2018, according to the International Telecommunication Union (ITU).\textsuperscript{1} There were 2.09 million mobile subscriptions at the end of 2018, a penetration rate of 139 percent. Broadband penetration was at 144 percent, or 2.16 million subscriptions, of which 91.5 percent consisted of mobile broadband.\textsuperscript{2}

Internet speeds have increased in recent years. The current average download speed is 37.3 Mbps; 74 percent of files are downloaded with a speed exceeding 10 Mbps, according to a 2017 report from Bahrain’s Telecommunications Regulatory Authority (TRA), the most recent available.\textsuperscript{3} A 2016 audit by the TRA found that 100 percent of the population was within reach of 3G and 4G mobile networks.\textsuperscript{4} Batelco, a state-controlled ISP, began offering “superfast” 500 Mbps speeds to residential subscribers that year,\textsuperscript{5} while 4G LTE mobile subscriptions have been available since 2013. In February 2019, provider VIVA Bahrain announced that it was ready launch 5G networks in various areas of the country.\textsuperscript{6}

Internet access is widely available in schools, universities, shopping malls, and in coffee shops—the latter providing a space for people to conduct personal work and study while connecting to complimentary Wi-Fi.
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?

Access to the internet is affordable for the majority of the population. Prices for mobile broadband are among the lowest in the region, with one provider, for example, offering 10GB per month for 7 Bahraini dinars ($19).1 Fixed-line broadband subscriptions with a 20 Mbps connection cost 21 dinars ($55) per month, less than 1 percent of the average Bahraini’s monthly income, with similar prices for mobile internet.2 Packages with fewer calls and data—for example, 6 dinars ($17) for 6GB per month—are affordable to Bahrain’s many low-wage migrant workers.3 Although these packages have no content limitations, the more expensive ones offer higher speeds.

The government provides free computer training programs, which had served nearly 17,000 citizens by September 2017, the most recently available data.4

• 1. TRA, “Bahrain Telecom Pricing International Benchmarking ”, slide 13,


A3 0-6 pts
Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity? 46

Although there is no centralized internet backbone in Bahrain, all ISPs are indirectly controlled by the government through orders from the TRA (see A5). Service providers connect to numerous international cables and gateways provided by Tata, Flag, Saudi Telecom, and Etisalat, among others, making the country less prone to unintentional internet outages.1 The TRA is working with telecom companies to establish the National Broadband Network (NBN), which is supported by a single fixed fiber-optic network.2 The TRA aims to have the NBN ready in 2019 (see A4).3

No cases of connectivity restriction were observed during the coverage period of this report. The most recent restriction lasted for over a year, from June 23, 2016 to July 30, 2017, when authorities implemented an “internet curfew” in Diraz after security forces besieged the town following a sit-in around the house of Shiite cleric Issa Qassem. The sit-in continued until May 23, 2017, when a violent crackdown left five dead and dozens injured.4

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

There are some obstacles to service providers seeking to enter the market, related primarily to acquiring the approval of various government bodies, and installation of the required systems that facilitate government content controls and monitoring.

Batelco, Zain, and VIVA are the three mobile phone operators, and also serve as the main ISPs. As of March 2019, the TRA was not accepting applications for mobile licenses, while ISP license applications remained open. In total, around 13 ISPs operated at the end of 2018. The government has a controlling stake in the largest ISP, Batelco, while other ISPs are owned by investors from the private sector, including non-Bahraini investors.

The requirements for establishing a new ISP are published by the TRA and Ministry of Commerce on their websites, and include the submission of a “lawful access implementation plan” that would allow security personnel to access subscribers’ data (see C6). The initial registration fee is relatively inexpensive, though operators also need to purchase the filtering system mandated by the TRA (see B1). Approval by the General Directorate of Criminal Investigation is also required. Both the infrastructure and personnel behind the ISP must be situated in Bahrain.

In April 2019, the TRA announced that it had reached the final consultation stages of its plan to establish a national fiber-optic broadband network, which will allow all service providers to share fiber-optic infrastructure built by Batelco. The plan includes splitting Batelco into two entities: one that will continue its retail services,
and another that will become the National Ground Cables Company (NBNetCo BSC), which will own the infrastructure and provide wholesale services to the licensed telecom operators. The splitting process is being monitored by a committee that includes members of the MOI, National Security Apparatus (NSA), and the Defense Force.

4. SIJILAT 2.0, Commercial Registration Portal, accessed October 8, 2019, https://www.sijilat.bh see snapshot of the requirements to get a Class License for Internet Services on https://drive.google.com/file/d/1Ik8008bacq5KhfkccrzF5z9yAeOTW0FP/view.
Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

Bahrain’s national regulatory bodies are in effect controlled by the monarchy. In the past, they have revoked licenses of operators that failed to install monitoring and filtering systems required by government authorities, and are indifferent to user complaints about internet controls.

Mobile phone services and ISPs are regulated by the TRA under the 2002 Telecommunications Law. The TRA is responsible for licensing telecommunication providers and for developing “a competition-led market for the provision of innovative communications services, available to all.” The Information Affairs Authority, which regulates the press, merged with the Ministry of Information Affairs (MIA) in December 2016.

Although the TRA is theoretically an independent organization, in practice its members are appointed by the king, based on cabinet approval, and through a royal decree published in the official gazette. As of March 2019, one of four board members and two members of the executive management were part of the royal family.

There have been no reported instances of ISPs being denied registration permits. However, in February 2016, the TRA revoked the license of the small mobile and fixed-line provider 2Connect. Among other issues, the company had failed to “provide a lawful access capability plan” that would allow security forces to access metadata about communications sent over its network. In December 2017, the TRA revoked the license of another small ISP, Bahrain Broadband, following a notice period, for failure to comply with several TRA regulations; these included failure to implement the unified technical solution for filtering and blocking, and failure to remain continuously connected to the central management system (see B3).

During the 2016–17 “internet curfew” in Diraz, no action was taken by the TRA to address consumer complaints about the shutdowns, despite widespread criticism from the media and nongovernmental organizations (NGOs).

- 2. In June 2013, Mohamed al-Rumaihi was named President of the IAA,
replacing Fawaz al-Khalifa who remained Minister of State for Telecom.


**B Limits on Content**
The government warned citizens from following “malicious” social media accounts, threatening legal action, in addition to claiming calls to boycott the November 2018 election came from outside the country. Numerous websites continued to be blocked, various online content was removed by social media users due to legal pressure and organized user reporting, and self-censorship remained high.

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

Authorities ramped up censorship after the 2011 prodemocracy protests, in which online media played an important role, and heavy-handed censorship has persisted since. Political content is widely blocked. While YouTube, Facebook, Twitter, and international blog-hosting services are freely available, authorities have blocked a number of messaging and livestreaming apps.

In December 2018, the website of the independent Bahrain news outlet Awal Online was blocked, one month after its launch.1 The news site, operated by anonymous editors, said the block occurred in the wake of critical reporting on a long-term minister. In March 2019, their Twitter account was temporarily suspended2 (see B2).

In May 2017, authorities blocked several websites, including the Qatari outlets Al-Jazeera, Al-Sharq, and Al-Raya, after Bahrain, Egypt, Saudi Arabia, and the United Arab Emirates (UAE) cut diplomatic ties with Qatar.3 Additionally, in June 2016, authorities blocked the communications app Telegram, which was popular among independent media, members of the political opposition, and protest groups in Bahrain. Both the app and its website remained blocked at the end of the coverage period of this report.4 Other blocked websites include the Arab Network for Human Rights Information (ANHRI); the Bahrain Center for Human Rights (BCHR); and Al-Quds Al-Araby, a London-based newspaper.5 Bahrain Mirror, a popular news site, also remains blocked.
Some mobile livestreaming services that were popular in 2011 remained blocked during the coverage period, including Ustream and Bambuser.6 A crowdsourced list of 367 blocked websites indicated that 39 percent of sites blocked as of August 2018 were political in nature, while 23 percent related to the use of tools to bypass blocking and censorship, such as anonymizers and web proxies.7

In August 2016, the TRA ordered all telecommunications companies to employ a centralized system for blocking websites managed by the TRA.8 The order is related to a US$1.2 million contract awarded in 2016 to Canadian company Netsweeper to provide a “national website filtering solution.”9 Netsweeper has since been identified on nine ISPs in the country, and filters political content on at least one.10 A report from November 2015 indicated that more than 85 percent of Bahraini websites are hosted outside of the country,11 despite excellent infrastructure. Even if they are blocked, websites hosted overseas are less vulnerable to being removed at the behest of the government and remain accessible to Bahrainis with access to censorship circumvention tools.

6. These sites include bambuser.com, ustream.tv, and other websites that stream directly to Twitter like twitcasting.tv, see, Bahrain Freedom Index (blog), https://bahrainindex.tumblr.com/post/148926421634/live-streaming-websit....
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?

Content seen as critical of the government is regularly removed from websites.

In March 2019, the Ministry of Housing removed several videos from its Instagram account that featured the minister of housing arguing that a small housing unit is only small if people view it as such. The removal came after the videos become viral and attracted sarcasm and criticism.1 Parts of recordings of sessions of the Shura Council, the upper house of parliament, have been removed by the council channel’s admin before being uploaded to its official YouTube Live channel. For example, removed from a March 3, 2019 recording was footage of a councilmember’s controversial remarks regarding the relationship between the village of Ma’ameer, and a large adjacent industrial area in which he owned a business.2 Removed from a June 2018 video was a representative calling opponents of a new retirement law “psychos.”3 The same statement of the councilmember was also removed from the website of a local newspaper, Al-Ayam.4
In July 2018, YouTube removed a video of a verbal attack against a Bahraini cleric who had visited Israel. The video was removed around four hours after its publication and after it had received 32,000 views. YouTube did not provide a reason for the removal.

Users exploit platforms’ reporting mechanisms to remove comments critical of authorities and achieve the suspension of accounts operated by activists and independent journalists. In March 2019, the Twitter account of independent online news site Awalonline was temporarily suspended due to organized user reporting (see B1). In February 2019, Instagram closed the account of Yousef al-Jamri, an online activist; earlier, in October 2018, likely due to user reporting, a video of Hezbollah’s leader commenting on the political situation in Bahrain was removed from al-Jamri’s account, with violations of community guidelines cited as cause. Additionally, the Instagram account of journalist Hani al-Fardan was suspended in December 2018 due to organized user reporting.

According to transparency reports, neither Google nor Twitter removed any content based on requests from the Bahraini authorities. Twitter did receive two removal requests in the first half of 2018, but did not withhold any content.

Authorities employ a variety of other, more heavy-handed tactics to force the removal of online content. Through arrests, prosecutions and torture, security forces have coerced many online forum moderators to permanently shut down their websites. During the arrest of columnist Ibrahim al-Sheikh in April 2019 (see C3), seven tweets were removed from his account, although it is unclear by whom. After being briefly detained in the same month, former member of parliament Mohammed Khalid deactivated his Twitter account for several weeks, before reactivating it as a private account (see C3). His lawyer, Mohammed al-Othman, had twice deactivated his Twitter account in the same month before ultimately restoring it.

1. @NabeelNowairah, Twitter post, March 17, 2019, https://twitter.com/NabeelNowairah/status/1107301312759324673; @Manamavoice, Twitter post [in Arabic], March 17, 2019, https://twitter.com/manamavoice1/status/1107286208563036161; @Manamavoice, Twitter post [in Arabic], March 17, 2019, 19 (see C3). His lawyer, Mohammed al-Othman, had twice deactivated his Twitter account in the same month before ultimately restoring it.20

• 3. @YusufAlJamri, Twitter post [in Arabic], June 14, 2018, https://twitter.com/YusufAlJamri/status/1007251780537856001.


• 7. 15 Twitter accounts were temporarily or permanently shut down in November 2018 to government supporters reporting them for violating the platform’s policies.

• 8. @AwalOnline, Twitter post [in Arabic], March 2, 2019, https://twitter.com/Awalonline/status/1101877006571134977 and “It is required that the Awal Newsite does not stand on its feet,” [in Arabic] Awalonline, March 2, 2019, https://perma.cc/7QKM-PY2Q.


• 10. @YusufAlJamri, Twitter post [in Arabic], October 13, 2018, https://twitter.com/YusufAlJamri/status/1051072316900339712.


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

The decision-making process and government policies behind the blocking of websites are not transparent. Multiple state organizations, including the MIA and the MOI, can order the blocking of a website without a court order. The MIA blocks websites that violate articles 19 and 20 of the Press Rules and Regulations, which prohibit material judged as “instigating hatred of the political regime, encroaching on the state’s official religion, breaching ethics, encroaching on religions and jeopardizing public peace or raising issues whose publication is prohibited by the provisions of this law.” The publication of false news is deemed a crime according to article 70 of the same law.

Authorities regularly send updated lists of blocked websites to ISPs, which are instructed to “prohibit any means that allow access to sites blocked.” Licenses of ISPs may be revoked by the TRA for failing to cooperate with the MIA’s blocking
The government’s frequently updated list of blocked websites is not available to the public, and site administrators do not receive notifications or explanations when their websites are banned. When trying to access a blocked site, users are only informed that the website has been “blocked for violating regulations and laws of Kingdom of Bahrain.” Clicking the link to a government website on which unblocking requests can be made leads to an error message.

There are no official regulations outlining an appeals process for content restriction, and, in absence of official publications of blocking orders, it is difficult to appeal through the court system. A 2009 MIA blocking order stated that no site could be unblocked without an order from the information minister.

Website administrators can be held legally responsible for content posted on their platforms, including alleged libel. In February 2016, the Interior Ministry stated that WhatsApp group administrators may be held liable for spreading false news if they fail to report incidents that occur in their group. The dissemination of false news that damages national security or public order is a criminal offense punishable by up to two years in prison.

Do online journalists, commentators, and ordinary users practice self-censorship?

Internet users exercise a high degree of self-censorship. Most people use pseudonyms on Twitter, online forums, and comment sections, for fear of being targeted by the authorities, or share content privately on social media instead of publicly. Even opposition news sites based outside Bahrain rarely publish the names of their editors. Investigations of users’ online activities have been launched at workplaces and universities.

Activists often stop tweeting following detentions and interrogations, and those who return to Twitter after being detained frequently avoid controversial subjects (see C7), including direct criticism of the king and other subjects that the MOI warns against discussing (see B5). In May 2019, exiled journalist Adel Marzooq said he lost 180 followers on Twitter days after the MOI described his account as malicious, and warned users not to follow or promote his messages (see C7). In April 2019, tweets about the takeover of public land in Arad by some royal family members stopped after several users who had criticized the events received summonses (see C3).

Self-censorship on Twitter in 2019 had become acute, with users expressing increasing fear of facing prosecution for discussion of anything beyond sports and lifestyle topics and political views in line with that of the regime. Mohsen Alsaffar, a Bahraini satirical writer, caustically asserted in April 2019 that “before posting any tweet, one must present it to a lawyer to ascertain its legal status, and to a cleric to ascertain its religious status, and to a diplomat to ensure that it is in accordance with international norms, and to a security expert to make sure it doesn’t support terrorism, and to an economist to make sure it does not destabilize the country's economy.”

4. “Activists announce their retirement from political and human rights...


7. @BahrainMirror, Twitter post [in Arabic], April 22, 2019, https://twitter.com/BahrainMirror/status/1120381829427679236.


9. @mohsenalsaffar, Twitter post [in Arabic], April 17, 2019 https://twitter.com/mohsensaffar/status/1118743538781437952.

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?

Government authorities and progovernment trolls work effectively to manipulate the online information landscape in Bahrain.

Authorities issue official statements warning against the discussion of certain subjects and the “misuse” of social media.1 In May 2019, the cybercrime directorate of MOI declared the accounts of several Bahraini activists and journalists accounts to be malicious,2 and a few days later sent SMS messages and tweeted to users to warn them that following “malicious” social media accounts could result in prosecution3 (see C7). In June 2018, the MOI warned against reposting a resurfaced video from 2011 of a “war dance” by a group of naturalized Bahraini citizens of Arab origins,4 saying that sharing of the video amounted to attempts to “incite sedition and disturb the social peace,” and warning that legal actions would be taken.5
Research from 2013 revealed connections between the Bahraini government and “extremist” accounts on Twitter and Facebook, which advocated violence against both the government and protesters. It was also revealed that the government impersonates opposition figures on social media in order to send malicious links, such as IP trackers, to anonymous government critics that can be used to identify and prosecute them.

Organized progovernment trolls have been active on Twitter since 2011, when hundreds of accounts suddenly emerged to collectively harass and intimidate online activists, commentators, and journalists who voiced support for protests and human rights; these efforts have been moderately effective in silencing or reducing the activity of opposition voices both inside Bahrain and abroad. Trolls have also played a role in spreading disinformation aimed at distorting the image of protesters, exacerbating conflict, or discrediting valid information posted on social networks. Twitter accounts impersonating users in prison were active as of August 2018 and were interacting with opposition supporters.

Prior to parliamentary elections in November 2018, some citizens received text messages that their names had been removed from the electoral register, implying they did not need to go to the polls. The government denied sending the messages, and the MOI alleged that while some were sent from within Bahrain, 40,000 others were sent from Iran in an attempt to disrupt the electoral process. Moreover, the MOI alleged that some candidates had received threats from social media accounts run from Iran by Bahraini political groups, such as the banned opposition group al-Wefaq, to persuade them to drop out of the race. In another statement, the MOI claimed that all social media accounts and websites calling to boycott the elections were run by users in Iran, Iraq, and Lebanon, adding that citizens should seek out information from reliable sources and ignore these calls. (Al-Wefaq and other opposition groups had called for a boycott of the polls.)

Twitter accounts from Saudi Arabia and the UAE have played a role in creating several trending hashtags about Bahrain, including one Arabic hashtag (“#Fire of Bahrain oil pipelines”) that blamed “terrorists”—a term often used to describe antigovernment protesters—for starting a fire in the oil pipelines. The hashtag originated from a Saudi-based account in November 2017 and reached many users in Saudi Arabia.

• “MOI: legal action against anyone who abuses the use of social media and


Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

Regulatory restrictions limit the ability of users to publish online content, while government censorship creates indirect economic constraints that leaves many outlets dependent on personal funding.

Newspapers must obtain licenses from Bahrain’s mass media directorate in order to disseminate electronic media on websites or social media, according to Decree 68/2016. The law does not detail what criteria is used to grant or renew the one-year license. Furthermore, outlets must provide a list of their social media accounts and website addresses, as well as the names of those who oversee them as part of the license application, exposing employees to possible monitoring and coercion. Under the existing press law, media professionals face six months of imprisonment and/or a fine of 5,000 dinars ($13,180) for publishing without a license.

Under Decree 68/2016, newspapers may not post videos over two minutes in length and are forbidden from live streaming video. The law also stipulates that electronic media must reflect the same content as their printed counterparts, limiting multimedia content.

There are some government restrictions on online advertising, but several opposition websites continue to operate nonetheless. While it is difficult for blocked websites to secure advertising, some popular sites such as Bahrain Mirror are able to operate with limited resources, and are often self-funded.


B7 0-4 pts
Does the online information landscape lack diversity?
The internet remains the main source of information and news for many Bahrainis, with many people getting much of their news through Twitter and Facebook. However, only outlets that operate from outside Bahrain can report on local politics freely, and many independent foreign-based sites are subject to blocking within Bahrain (see B1).

Despite the government’s stringent information controls, blocked opposition websites and Bahraini news outlets based outside the country continue to receive traffic from users within Bahrain through the use of proxy services, dynamic IP addresses, and virtual private network (VPN) applications. The government used to block access to Google Translate and Google cached pages, which could be used as circumvention tools, but these were found to be accessible in May 2019.

- 2. Sites were verified accessible through browser from Bahrain on Batelco and Viva networks on May 3, 2019

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

Activists rely heavily on digital tools, particularly social media, to draw attention to protests and human rights violations. However, due to the threat of arrest, prosecution, and other consequences for online activity, many users are extremely wary of participating in political discussions over social media. Authorities have also blocked some tools used to mobilize or campaign, such as Telegram (see B1).

Even as its users increasingly self-censor, Twitter remains a key platform for mobilization. Users often report on the status and conditions of various detainees’ arrests and detentions and calls for their release. Additionally, the Coalition of February 14 Youth protest movement continues to use social networks to organize protests and bring international attention to local causes. A Twitter campaign started in August 2018 using the hashtag #Forged_Degrees_in_Bahrain (in Arabic) exposed information about several officials and private-sectors actors who earned bogus degrees. After gaining traction on social media, traditional media outlets
began discussing the controversy. The prime minister ordered an investigation, though few of the officials were penalized.

In June 2018, Bahrainis used Twitter to oppose the government’s attempt to change the retirement law, a rare occasion of relative unity around a single cause, according to one source. While the change was initially approved, the king acknowledged the criticism expressed over “different channels of media,” and instructed the government to review the law.

2. See, for example, BahrainDetainees (@FreedomPrayers), Twitter Account, https://twitter.com/FreedomPrayers/lists/bahraindetainees.
Violations of user rights in Bahrain were rampant, with at least 21 users arrested, detained, or prosecuted over the coverage period for their online activities. Those targeted included progovernment and nonpartisan figures, as well as a popular actor and one of the country’s most prominent human rights defenders. Some detainees were subjected to torture. A Citizen Lab report showed that Bahrain may have used the powerful spying software, Pegasus. Regulations requiring all mobile subscribers to verify their identity through fingerprinting began to be enforced during the reporting period.

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?

A variety of laws place restrictions on free speech, and the compromised judiciary does not uphold protections that do exist.

According to article 23 of the constitution, freedom of expression is guaranteed, “provided that the fundamental beliefs of Islamic doctrine are not infringed, the
unity of the people is not prejudiced, and discord or sectarianism is not aroused.”

Article 26 states that all written, telephonic, and electronic communications “shall not be censored or their confidentiality be breached except in exigencies specified by law and in accordance with procedures and under guarantees prescribed by the law.” The Press and Publications Law of 2002 promises free access to information “without prejudice to the requirements of national security and defending the homeland.” Bahraini journalists have argued that these qualifying statements and loosely-worded clauses allow for arbitrary interpretation and, in practice, the negation of the rights they claim to uphold.

The judicial system in Bahrain is neither independent nor fair. Serious crimes have been committed against internet users, including torture (see C7), and impunity for these offenses prevails.

- **1.** Constitution of the Kingdom of Bahrain, art. 23, http://www.shura.bh/ar/legislativeresource/constitution/pages/default.a....
- **2.** Constitution of the Kingdom of Bahrain, art. 26, http://www.shura.bh/ar/legislativeresource/constitution/pages/default.a....
- **5.** “In Bahrain, the two-faced nature of impunity: Oppressors rewarded, activists suffer,” IFEX, February 12, 2019, https://ifex.org/in-bahrain-the-two-faced-nature-of-impunity-oppressors....

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

Multiple laws, including the penal code and terrorism laws, criminalize free speech and online activities. Criminal penalties for online speech are currently enforced
under the 2002 Press and Publications Law, which does not specifically mention online activities, but has been applied to digital media. The law allows for prison sentences from six months to five years for publishing material that criticizes Islam, its followers, or the king, as well as content that instigates violent crimes or the overthrow of the government. Article 70 of the Press and Publications Law penalizes certain types of content, including “false news,” that undermines public security and criticism of presidents or states with which Bahrain has diplomatic ties. In addition, the 2002 Telecommunications Law contains penalties for several online activities, such as the transmission of messages that are offensive to public policy or morals.

Sentences can be longer than what is mandated by the Press and Publications Law if users are tried under the penal code or terrorism laws—especially in relation to social media, where the Press and Publication Law is not used. Under the penal code, any user who “deliberately disseminates a false statement” that may be damaging to national security or public order may be imprisoned for up to two years. Under article 309 of the penal code, any “expression against one of the recognized religious sects” or ridicule of their rituals may be punished by a fine of 100 dinars ($260) or a prison term of up to one year. In May 2019, the king ratified an amendment to article 11 of the terrorism law that criminalizes propagating, glorifying, justifying, favoring, or encouraging acts that constitute terrorist activities, with a penalty for up to five years in prison and a fine of between 2,000 and 5,000 dinars ($5,200 to $13,200). Following the approval of this amendment, activists and lawyers have warned social media users that acts of commenting, retweeting, liking, or forwarding could meet the criteria of the above-mentioned crime.

In February 2018, the cabinet endorsed a draft amendment to the penal code that would increase the maximum prison sentence for posting private news, comments, or images deemed defamatory from one year to three years, and would increase the maximum fine from 500 to 10,000 dinars ($1,320 to $26,350). However, it was still under discussion at the Council of Representatives (the lower house of the National Assembly) at the end of the reporting period.

In April 2017, the king approved a constitutional amendment to allow civilians to be tried in military courts. When military courts last operated in this manner, during a state of emergency in 2011, judges handed down prison sentences to bloggers that ranged from 15 years to life. In addition, the public prosecutor has begun using
a legal provision that calls for the prosecution of parents when their children are arrested for criminal activities including “misusing social media.”

The 2014 computer crimes law criminalizes the illegal access of information systems and possession of pornographic electronic materials.

- **8.** Video post by Lawyer Faten Hadad (@fatenhaddad) [Arabic] warns from tweeting, commenting or sharing screen of anything related to the terrorists acts that could be a crime, Faten Haddad, Instagram post [in Arabic], May 25, 2019, https://www.instagram.com/p/Bx5kS02A5ZG/?igshid=glmvpn0n7nr0; Ali Fadhel (@AliFadhel87), Twitter post [in Arabic], May 25, 2019, https://twitter.com/AliFadhel87/status/1132392262980317188.
- **10.** “Shura Council approves bill to impose 20,000 dinars for defamation on
C3 0-6 pts
Are individuals penalized for online activities?  16

Individuals are frequently detained and prosecuted for online activities, and those convicted typically receive harsh sentences. Between June 2018 and May 2019, at least 21 individuals were arrested, detained, or prosecuted for their online activities, and while some were still on trial as of May 2019, 52 months’ worth of prison sentences were collectively passed down on five Bahraini users during this report’s coverage period. (Two of them, who received one- and six-month sentences, respectively, were allowed to exchange their prison sentence with full or partial noncustodial sentences.)

The Electronic Crimes Directorate publishes official statistics on cybercrime cases each year, although it is difficult to determine which cases are related to political, social, or religious speech protected under international law. There were 292 cases of “misuse of the telecommunication mediums” brought forward in 2018, 127 of which were prosecuted.¹

Nabeel Rajab, one of Bahrain’s most prominent human rights defenders, the president of the Bahrain Centre for Human Rights, and an active Twitter user,² has been in and out of prison since 2012 for his online speech.³ In December 2018, he lost his final appeal,⁴ as the Supreme Court held up a February 2018 sentence of five years in prison, after a trial that lasted more than a year, on charges that included “spreading false news during a time of war,” “insulting a neighboring country,” and “insulting a statutory body.”⁵ The charges were based on 2015
Twitter posts, including retweets of posts by human rights organizations, about the Saudi-led coalition airstrikes in Yemen and the alleged torture of detainees at Jaw prison. The court handed down the sentence despite the prosecution’s failure to prove Rajab’s ownership of the Twitter account in question. Separately, in March 2019, opposition leader Ebrahim Sharif was sentenced to six month’s imprisonment on charges of “publicly insulting a foreign country…or its leader” over a December 2018 tweet in which he called on Sudan’s then president, Omar al-Bashir, to resign. The sentence was later suspended after he paid a 500 dinar ($1,300) fine.

There were several cases of interrogations and prosecutions related to the November 2018 elections. On November 13, 2018, Ali Rashed al-Ashseeri, a former member of parliament and member of the now-dissolved opposition group al-Wefaq, was summoned for interrogation by the public prosecutor over a tweet posted on November 8 saying he and his family would boycott the elections. He was immediately arrested and charged with “violating the referendum and jamming the electoral process.” He was released on bail days later, but ultimately sentenced to a month in prison and a 500 dinar ($1,300) fine. In April 2019, with 15 days left to serve, his sentence was commuted to 21 days of community service. In January 2019, a man was sentenced to three months in prison for insulting the interior ministry after posting tweets in October that criticized the ministry’s assertion that Iran-run social media accounts were behind threats to candidates. Many other individuals were subject to arrests, fines, and prison sentences for online activity. In April 2019, lawyer Abdulla Hashim was among a number of people summoned for interrogation at the electronic crimes directorate over Twitter posts objecting to the takeover of public land in the town of Arad by some royal family members. In May, Hashim was detained following a second summons by the public prosecution, over charges of disseminating false news harmful to public order and misusing social media. He was released, though the charges were not dropped. Also in April 2019, progovernment columnist Ibrahim al-Sheikh was arrested and charged for broadcasting false news that would harm national security over Twitter posts including one promoting his article questioning activities of Saudi-led military forces in Yemen. He was released days later and subsequently published an apology to the army, and has not published again since. In March 2019, psychotherapist Sharifa Siwar was interrogated and later charged
with defamation, dissemination of false news, and misuse of telecommunication mediums after posting videos on her Instagram account of herself interviewing a school student about the trade and use of drugs at an intermediate girls’ school. She had not been arrested as of May 2019. In April 2019, former lawmaker Mohammed Khaled was arrested for alleging in a tweet that the drug case was not being investigated by local newspapers because the papers feared consequences from the “unmentionable person” who is behind the drug trade. He was released after several days and immediately closed down his Twitter account.

In December 2018, popular actor and producer Qahtan al-Qahtani was arrested and charged with defamation, insulting a regulatory body, and abusing telecommunications equipment after an electronic message he wrote that questioned the information minister’s knowledge of basic media work circulated on social media; he was released after a few days. In August 2018, cleric Mohamed Saeed al-Aradi was sentenced to six months in prison for insult crimes over tweets quoting a historical speech that was critical of the prophet’s companions, though the sentence was later changed to community service. In July 2018, an unidentified man was arrested for posting videos on Snapchat calling on the king to address poverty and the lack of social justice in Bahrain. And in June, Najah Ahmed Yousif was sentenced to three years in prison over charges of “engaging in social media activity to encourage the overthrow of the political system.” She had criticized Bahrain’s hosting of the Formula One race on Facebook and had been detained since April 2017. Moreover, her conviction was based on a coerced confession and allegations of torture and sexual assault (see C7).

At least eight other internet users are still serving prison sentences for earlier online activities, including Abduljalil Al-Singace, a human rights defender and blogger who has been serving a life sentence since 2011 on charges of possessing links to a terrorist organization aiming to overthrow the government, disseminating false news, and inciting protests against the government.

Separately, many prominent journalists have been barred from entering the country over their work.

2. Rajab was ranked the “most connected” Twitter user in Bahrain according to a survey, with over 260,000 followers as of May 2015. See: Wamda, How the Middle East Tweets: Bahrain’s Most Connected Report December 3, 2012, https://www.wamda.com/2012/12/how-the-middle-east-tweets-bahrain-s-most...


6. Adam Rajab (@Adamnabeel), Twitter post, “Photos from the case file of sample tweets over which my father Nabeel Rajab is being tried, which may make him spend five years in prison,” June 4, 2018, https://twitter.com/Adamnabeel/status/1003877002263388160.


• **26.** Yusuf AlJamri (@YusufAlJamri), Twitter post [in Arabic], snapshot of the now deleted tweet – Translation “Most of the columnists in our local newspapers are [not reporting] about the Madinat Hamad case despite the seriousness of the case and they seem to be afraid of [the unmentionable person],” April 16, 2019, https://twitter.com/YusufAlJamri/status/1118206884383793152; https://perma.cc/RPJ7-Q26Z.

• **27.** Hani Alfardan (@manamavoice1), Twitter post [in Arabic], April 22, 2019, https://twitter.com/manamavoice1/status/1120341824848187396.


• **35.** “Detained blogger Abduljalil Al-Singace on hunger strike,” Reporters
C4 0-4 pts
Does the government place restrictions on anonymous communication or encryption?

The government restricts the use of many VPNs, imposes onerous registration requirements on mobile phone users, and has sought to uncover the identities of anonymous or pseudonymous users in order to prosecute them.

The TRA requires users to provide identification when registering new telecom connections, and the government prohibits the sale or use of unregistered prepaid mobile SIM cards. In July 2017, a TRA regulation that allows individuals to purchase no more than 10 prepaid SIM cards from a single service provider came into force. Under the regulation, people must be physically present when registering SIM cards directly with service providers, who must verify the identity of all subscribers on an annual basis, including through fingerprinting, which is justified as a security measure to help solve crimes. Service was cut for unregistered users in June 2018 for postpaid services, and has been cut on June 2019 for unregistered users of prepaid services.

Anonymous government critics have been sent malicious links in order for authorities to ascertain their identity and take legal action against them (see B5).

Tech-savvy activists use VPNs to conceal their identity. Access to websites of popular VPNs like Hotspot Shield, Express VPN, and the Tor Project are blocked, which makes it difficult to download their client applications. However, the connectivity and functioning of these VPN clients and Tor browsers remained unaffected during the coverage period.
A 2014 computer crimes law (60/2014) criminalizes the encryption of data with criminal intentions. Observers contend that “criminal intentions” could include criticism of the government.


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

State surveillance of online activities is widespread. Several reports have documented the government’s use of spyware against dissidents. In October 2018, it was revealed that Bahrain had purchased espionage and intelligence-gathering software from private companies, including a system from Verint used for collecting information from social networks. Additionally, training was provided to members of Bahraini intelligence on these systems’ use.1

In September 2018, a Citizen Lab report showed that Bahrain may have used the spying software Pegasus, developed by the Israeli company NSO Group. After the user clicks on an exploit link, Pegasus is covertly installed on their phone, granting the operator access to information including passwords, contacts, text messages,
and live voice calls from messaging apps, as well as the ability to open the camera and microphone. Citizen Lab identified efforts that may have targeted the persecuted Shia majority and members of the Coalition of February 14.2

In October 2018, a month before the parliamentary elections, the MOI announced that it was monitoring phone messages, likely in the form of texts or voicemails that promoted an election boycott, and would take legal action against those involved (see C3).3

In March 2018, it was reported that Bahrain purchased $544,000 worth of British surveillance equipment between 2015 and 2017.4

A Cyber Safety Directorate at the Ministry of State for Telecommunications Affairs was launched in November 2013 to monitor websites and social media networks, ostensibly to “ensure they are not used to instigate violence or terrorism and disseminate lies and fallacies that pose a threat to the kingdom's security and stability.”5 Officials had earlier created a unit to monitor social media and foreign news websites to “respond to false information that some channels broadcast” in 2011.6

In January 2017, the government ratified the Arab Treaty on Combating Cybercrime, a set of standards developed to stem the misuse of telecommunications devices, financial fraud, the promotion of terrorism, and access to pornographic content online. While Bahrain passed a computer crimes law containing many of the provisions in 2014, the treaty establishes new rules on the retention of user data and real-time monitoring of activities, as well as a mechanism for sharing information between signatories to help combat transnational crime. The lack of strong human rights standards in the treaty may increase the scope for privacy infractions once it is transposed into local law.7

Bahrain lacks a privacy law. While a personal data protection law was introduced in July 2018 (see C6), article 2.4(b) exempts national security-related data processing undertaken by the Interior Ministry, national security apparatus, defense ministry, and other security services.8

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

Since 2009, the TRA has mandated that all telecommunications companies keep a record of customers’ phone calls, emails, and website visits for up to three years. The companies are also obliged to provide security forces access to subscriber data upon request from the public prosecution, while the provision of the data content requires a court order.1

In order to receive an operating license (see A5), the provider must develop a
“lawful access capability plan” that would allow security forces to access communications metadata. The provider 2Connect had its license revoked in February 2016 due to its failure to set up this plan.

Cybercafés are also subject to increasing surveillance. Oversight of their operations is coordinated by a commission consisting of members from four ministries, who work to ensure strict compliance with rules that prohibit access for minors and require that all computer terminals are fully visible to observers.2

According to company transparency reports, Bahrain submitted one user data request to Google,3 six user data requests to Twitter,4 and three user data requests to Facebook5 in the first half of 2017. The companies refused all the requests. No requests were made in 2018. Information on local providers complying with the state’s requests for users’ data is not made public.

Bahrain introduced a personal data protection law similar to the European General Data Protection Regulation (GDPR) in July 2018, scheduled to be implemented in August 2019, that delineates the requirements for entities collecting, processing, and storing personal data, including getting consent from the user and informing them that data is being collected. It is unclear what its enforcement might look like.


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?
Violence and torture against online activists and journalists at the hands of authorities is common in Bahrain.

In June 2018, Najah Ahmed Yousif was sentenced to three years in prison based on a coerced confession (see C3). She was reportedly tortured and sexually assaulted during her interrogation. A woman who was arrested in May 2019 for insulting the king over social media was reportedly subject to abuse during detention that led to her transfer to a psychology hospital (while still under detention).

Numerous online activists have fled Bahrain, including blogger and founder of the Bahrain Online forum Ali Abdulemam, who was detained and tortured in 2010 and, in a separate case in 2011, sentenced to 15 years imprisonment by military court; blogger Mohamed Hasan, who was tortured during a 2013 detention and fled in 2014; and Twitter activist Hussein Mahdi, also tortured while being detained in 2014. In August, 2017, online activist Yousif Al-Jamri fled Bahrain after facing increasing intimidation by the NSA following his publication of a video alleging that he was subjected to physical and psychological torture at the NSA, threatened with rape and reprisals against his family, and forced to insult religious figures he reveres.

Bahraini activists living abroad are subject to online threats from people affiliated with the security apparatus. In June 2018, an Instagram account appearing to belong to an MOI officer sent messages to activist Sayed Yousif Almuhafdh, who is living abroad, that his brothers in Bahrain would be arrested unless he stopped working as an activist, closed his social media accounts within a day, and sent a video apologizing to the king of Bahrain. The same account sent a death threat to Bahrain-based human rights activist Ebtisam al-Saegh, and claimed they would release a video of the torture and sexual assault she was subjected to during her 2017 detention. A Twitter account with the handle @godkingcountry threatened to rape al-Saegh if she did not end her online activism.

In May 2019, the Interior Ministry accused people based in Iran, Qatar, Iraq, and Europe, as well as the activist Sayed Yousif Almuhafdh (in exile in Germany) and activist Hassan Abdulnabi (in exile in Australia) of running social media accounts that encourage sedition, and harmed public order and the image of Bahrain. It also added that their network received support from “e-cells” operating from inside the country, whose members had been identified and should expect prosecution. The
Interior Ministry also discouraged interaction with these networks.

In May 2019, the Interior Ministry tweeted that the Twitter account of Adel Marzooq, a Bahraini journalist in exile and chief editor of the Gulf House for Studies and Publishing, is “encouraging sedition between members of society.” It threatened to take legal actions against it and against whoever promote its messages.13 The threats came in response to Adel’s tweets about a conflict within the royal family over whether or not to remove the prime minister.14

The New Yorker reported in June 2018 that the PR firm Bell Pottinger provided its Bahraini clients with a list of the most effective dissidents and activists on social media “at a time when Bahraini officials were imprisoning and torturing people who spoke out against the regime.”15


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

Cyberattacks against both opposition and government supporters are common in Bahrain. In January 2019, the Twitter account of the progovernment newspaper Al-Watan was hacked by a group identifying as the Yemen Cyber Army. The hacker also posted messages against the Saudi coalition’s intervention in Yemen. In December 2018, the website of Bahraini newspaper Al-Bilad was hacked. Also in December, the WhatsApp account of human rights lawyer Mohamed al-Tajer was hacked, while on June 27, 2018, the opposition news website Bahrain Al-Youm was hacked by an actor identifying by the name the Saudi Cyber Army. In July 2018, the Twitter account @Emp_Bahrain shared that it was hacked and controlled by allies of the prime minister.

According to a 2018 Trend Micro report, in the first quarter of 2018 Bahrain was subject to 1.2 million ransomware attacks, 202,241 malware attacks, and 523 malicious URL attacks. In December 2018, a report by the Kaspersky Lab found that Bahrain was subject to almost 8 million cyberattacks in 2018, including phishing, ransom, and Trojan attacks.

Authorities observed more than 2 million malware attacks and 62 million malicious emails sent to government systems during 2018.

- 1. Hani Alfardan (@manamavoice1), Twitter post [in Arabic], January 8, 2019, https://twitter.com/manamavoice1/status/1082672831727587329
Country Facts

- **Freedom in the World Status**
  - Not Free

- **Networks Restricted**
  - No

- **Social Media Blocked**
  - Yes

- **Websites Blocked**
  - Yes

- **Pro-government Commentators**
  - Yes
Users Arrested

Yes

Previous Reports

• 2018 Report