

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	632
Land:	Sri Lanka
Kilde:	Freedom House
Titel:	Freedom on the Net 2020: Sri Lanka
Udgivet:	2020
Optaget på baggrundsmaterialet:	6. januar 2021



Freedom on the Net 2020

Sri Lanka

52
/100

PARTLY FREE

A. <u>Obstacles to Access</u>	12 /25
B. <u>Limits on Content</u>	22 /35
C. <u>Violations of User Rights</u>	18 /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

Internet freedom remained constrained in Sri Lanka. Although the government refrained from blocking social media or communications

platforms in 2020 as it had done in 2019 and 2018, the online space for free expression continued to shrink. Following November 2019 presidential elections, journalists and activists reported increased intimidation and harassment, contributing to self-censorship and a more fearful climate. New evidence suggests that government actors manipulate information across major platforms. Separately, COVID-19 brought more arrests for online activity as well as enhanced data sharing between service providers and military intelligence.

The coverage period marked a time of transition, with President Gotabaya Rajapaksa being elected in November 2019, on the strength of a campaign that promoted national security as a priority after a series of attacks at churches and hotels on Easter Sunday 2019. Previously, Sri Lanka had experienced improvements in political rights and civil liberties after the 2015 election of President Maithripala Sirisena, which ended the more repressive rule of Mahinda Rajapaksa, Gotabaya Rajapaksa's brother. However, under Sirisena, the coalition government was slow to implement a range of political reforms, including establishing meaningful transitional justice mechanisms needed to address the aftermath of a 26-year civil war between government forces and Tamil rebels, which ended in 2009. Sirisena's reputation as a democratic reformer was further tarnished by a constitutional crisis in 2018, in which he attempted to make unilateral moves that were blocked by the parliamentary majority and the courts. After taking office, Gotabaya Rajapaksa appointed his brother Mahinda, who was key to his victory, to serve as prime minister. After the coverage period, the Rajapaksas' ruling party, the Sri Lanka Podujana Peramuna, won a majority of seats in August 2020 parliamentary elections and secured enough support from allied parties to form a supermajority.

Key Developments, June 1, 2019 - May 31, 2020

- Unlike in 2018 and 2019, the government imposed no social media blocks or connectivity restrictions during the coverage period,

although it still retains control over internet infrastructure (see A3 and B1).

- Following the November 2019 election of Gotabaya Rajapaksa as president, journalists and activists reported an increase in self-censorship around political issues (see B4).
- A new report identified certain government agencies, politicians, and political parties that have coordinated cybertroop teams to manipulate information across major social media platforms (see B5).
- A growing number of people were prosecuted in retaliation for their online activities. In August 2019, the award-winning author and poet Shakthika Sathkumara was finally released on bail after being held since April for a short story he shared on Facebook. Ramzy Razeek, a commentator on political and social topics on Facebook, was also arrested in April 2020 and held in detention for at least a month (see C3).
- Amid the COVID-19 pandemic, government initiatives for contact tracing and quarantine compliance—including a new smartphone app and the retrieval by military intelligence of personal data from mobile service providers—raised privacy and surveillance concerns (see C5 and C6).

A. Obstacles to Access

Internet penetration in Sri Lanka continues to increase, but women have less access to the Internet and an urban-rural digital divide persists. The Telecommunications Regulatory Commission of Sri Lanka (TRCSL) continues to be led by political appointees, and has been brought under the Ministry of Defence, limiting its independence.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

4 / 6

Although internet access has increased in recent years, the speed and quality of service is inconsistent. There was a steady rise in the number of mobile broadband subscriptions during the coverage period, which reached over 11 million by December 2019, according to the TRCSL. ¹ The number of fixed broadband subscriptions increased slightly by the end of 2019, reaching over 1.5 million in December.

The government is interested in expanding internet access and digital infrastructure projects. Newly elected President Gotabaya Rajapaksa has laid out his plans to make Sri Lanka “digitally inclusive”; the plans include the development of a high-speed optical transmission system and fifth-generation (5G) mobile broadband countrywide, as well as the digitization of more government services using Internet-based technologies. ² The Information and Communication Technology Agency is also focused on improving and lowering the cost of access to the internet and other digital services. ³

Private companies are also working to expand service. In 2019, the internet service provider (ISP) Dialog Axiata had over 2,500 pay-to-use Wi-Fi hotspots around the country, ⁴ and spent a reported 28.6 billion rupees (\$157 million) on broadband and other infrastructure. ⁵ In February 2020, Dialog agreed to invest \$254.1 million (45.5 billion rupees) in information and communication technology (ICT) infrastructure, including expanding fourth-generation long-term evolution (4G LTE) networks and developing Wi-Fi and broadband networks. ⁶ Sri Lanka Telecom is also aiming to substantially expand its coverage during 2020 and 2021. ⁷ Meanwhile, Hutch invested \$200 million (36 billion rupees) in an effort to provide 4G nationwide during 2020. ⁸ During the reporting period, service providers moved toward offering 5G service. In June 2019, Dialog used a commercial 5G mobile set to achieve download speeds greater than 1.4 Gbps, while Mobitel reached speeds of 1.55 Gbps. ⁹ In January 2020, Sri Lanka Telecom said it was prepared to launch 5G services. ¹⁰

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?	
---	--

Mobile internet connectivity is affordable, although gender-based and urban-rural digital divides persist. In a survey, 25 percent of respondents said cost of data was a limiting factor in internet use. According to cable.co.uk's 2019 study of global internet prices, Sri Lanka's average monthly price for fixed-line broadband was \$27.4 (4,910 rupees). For comparison, mean household income in Sri Lanka was 62,237 rupees (\$341), according to the most recent Household Income and Expenditure Survey in 2016. ¹ Prices for mobile broadband vary. ² According to the International Telecommunication Union (ITU), Sri Lanka is ranked 21st out of 181 countries for affordability of mobile broadband, although its taxes for such services are the third-highest in the region. ³

The province with the highest percentage of households accessing the internet is the Western Province, the country's most populous, ⁴ where Colombo and other urban areas boast well-developed infrastructure. Government statistics for the first half of 2019 found about 43.4 percent of Western Province residents to be "computer literate," ⁵ a category that excludes those whose only digital literacy is through smartphones or tablets. By comparison, the national *digital* literacy rate, including those able to use any digital device, is 44.3 percent compared to a national computer literacy rate of 30.1 percent—showing the shift away from personal computers. ⁶

The civil war, which ended in 2009, delayed infrastructure development in the Northern and Eastern Provinces. However, the telecommunications infrastructure has improved in recent years, which has led to steady growth in internet usage. In 2019, 19.6 percent of Northern Province residents were categorized as computer literate. ⁷ Compared to urban areas, rural and up-country Tamil communities have significantly lower computer and digital literacy rates. ⁸

Schools with digital facilities often lack corresponding digital literacy programs. A government initiative to provide tablet computers to students

has been stalled since 2018. ⁹ In its current projects, ICTA mentions a “million tabs” program, which would give residents affordable access to tablets with educational content. ¹⁰ Only an estimated 40 percent of households with children have an internet connection, and 52 percent of households with children have a smartphone or computer, cutting many students off from e-learning initiatives. ¹¹

For a number of years, the ICTA has promoted digital literacy in rural areas by establishing community-based e-libraries and e-learning centers, ¹² though some local journalists have criticized aspects of the initiative. ¹³ In 2017, the Ministry of Education inaugurated the country’s first “cloud smart classroom,” a pilot project for digital interactive learning. ¹⁴ Those who participated in the cloud smart classroom reported higher attendance rates and performance. ¹⁵

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	4 / 6
--	--------------

Score Change: The score improved from 2 to 4 due to the government imposing no social media blocks or connectivity restrictions during the coverage period.

The government refrained from restricting connectivity and blocking social media platforms during the coverage period. However, certain measures introduced by the government—including the consolidation of several bodies under the Ministry of Defence’s purview—raised concerns over the government’s ability to order telecom operators to block social media platforms (see A5).

During the previous coverage period, the government blocked social media platforms repeatedly in April and May 2019 in the wake of the Easter Sunday suicide attacks at churches and hotels. ¹ For nine days directly following the attacks, Facebook, WhatsApp, YouTube, Instagram, Snapchat, and Viber were all blocked, as was at least one popular virtual private network (VPN). ²

The government had previously restricted connectivity in the Kandy district following communal violence in March 2018. In response to the violence, the Ministry of Defense ordered a nationwide block of Facebook, WhatsApp, Instagram, and Viber. ³

Sri Lanka has access to multiple international cables, but most of the landing stations for these cables are controlled by the majority state-owned Sri Lanka Telecom (SLT), giving the government control over internet infrastructure. ⁴ In August 2019, SLT launched the Xyntac brand, which planned investments in international submarine cable systems and data centers. ⁵ In February 2020, a new project to lay a submarine cable system between the Maldives and Sri Lanka was announced; a consortium of telecommunications companies including Dialog Axiata have come together to build the cable. ⁶

A4 0-6 pts

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

3 / 6

Sri Lanka's retail tariffs are among the lowest in the world, though the diversity of service providers is limited due to the dominance of some companies, particularly the majority government-owned provider SLT.

There are three ISPs in Sri Lanka, according to the TRC. ¹ SLT remains a key player in the ICT market, and the firm imposes price barriers by forcing competing service providers to lease connectivity from SLT, which charges high rates. ²

Dialog Axiata remains the largest mobile service provider, with nearly 14.9 million subscribers in 2019, ³ followed by Mobitel, a subsidiary of SLT, ⁴ which had over 9 million subscribers by the end of 2018. ⁵ Hutch had the third largest number of subscribers, with over 5.3 million reported in July 2019. ⁶ Airtel Lanka had 2.9 million subscribers as of December 2018. ⁷

In 2016, SLT announced that it would provide a global connectivity backhauling facility via Sri Lanka, thereby allowing the company to cross-

connect to other cable systems and increase capacity.⁸ In August 2018, the government removed telecommunications floor rates for call charges in hopes of increasing competition among service providers.⁹

The competitive nature of the market has led to some legal battles. In August 2018, for example, the Commercial High Court rejected Dialog's petition against SLT, which accused SLT of violating intellectual property rights.¹⁰

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?

0 / 4

The national regulatory bodies overseeing service providers lack independence, and frequently do not act in a fair manner. The TRC continued to be led by political appointees during the coverage period.

The TRC was established under the Sri Lanka Telecommunications (Amendment) Act, No. 27 of 1996. As the national regulatory agency for telecommunications, the TRC's mandate is to ensure the provision of effective telecommunications, protect the interests of the public, and maintain effective competition between service providers.

In December 2019, President Rajapaksa issued a gazette notification showing that several bodies—including the TRC, the Information and Communication Technology Agency of Sri Lanka, and Sri Lanka's Computer Emergency Readiness Team (SLCERT)—had been brought under the purview of the Ministry of Defence, a reorganization that heightened concerns about the TRC's independence and about potential government surveillance projects.¹ The TRC's new position under the Ministry of Defense had been announced previously, in March 2019, when then-president Sirisena issued a special gazette to that effect.²

The TRC has been criticized in the past for poor regulatory practices, lack of transparency in recommending whether a telecommunications provider should receive a license, and instances of preferential treatment.³

Analysts have asserted that spectrum allocation and refarming (the more efficient reallocation of spectrum) have been administered in an ad hoc manner, but over the years, procedural transparency has improved. ⁴ However, regulatory reforms to improve the TRC's performance and increase its independence are necessary.

During former president Mahinda Rajapaksa's regime, many of the TRC's interventions to restrict online content and pronouncements on strengthening internet regulations were partisan and extralegal. ⁵ In 2017, the Colombo High Court found former TRC chairperson Anusha Palpita and former secretary to Rajapaksa Lalitha Weeratunga guilty of misappropriating TRC funds for Rajapaksa's presidential campaign. They were sentenced to three years in prison and fined, but were released on bail pending their appeal of the verdict. ⁶ The appeal petitions were fixed for March 2020 ⁷ and in the interim, a travel ban imposed against Weeratunga was temporarily lifted to allow him to travel to India along with the President Gotabaya Rajapaksa. ⁸

Former president Sirisena largely chose political allies to head the TRC. The previous director general was P.R.S.P. Jayatilake; Jayatilake's brother was a member of Parliament and Sirisena ally who had written a book about the president. ⁹ In December 2019, Secretary to the Defence Ministry Major General Kamal Gunaratne was appointed chairman of the TRC, continuing the practice of the president giving the post to political associates. ¹⁰

B. Limits on Content

There were no blocks on social media or communications platforms during the coverage period, although several websites remain blocked. Some journalists and rights activists reported increasing self-censorship following the presidential election, with topics like the army, rights violations, land appropriation, and corruption being considered sensitive topics. Misinformation continued to distort online discourse. Separately, new evidence suggests that the government has coordinated cybertroop teams to manipulate information across major social media platforms.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?

4 / 6

Score Change: The score improved from 3 to 4 due to the government imposing no blocks on social media or communications platforms.

The government does not systematically block or filter websites and other forms of online content, although a few independent websites and other sites are blocked. Authorities have previously blocked social media and communications platforms.

Lankaenews remained blocked during the coverage period. The website was reportedly first blocked for publishing stories critical of the then-president Sirisena. ¹ Of 13 websites found to be blocked through a right to information request between 2015 and 2017, ² two were unblocked, while many of them had become inactive after being blocked.

During the coverage period, tests from the internet censorship organization OONI showed signs of “HTTP blocking” when trying to access sankathi24.com, a Tamil news site, and signs of “DNS tampering” when accessing teenhealthfx.com, a teen health, relationships and sexuality site, from domestic connections, suggesting that the sites may be blocked. ³ Both sites were inaccessible on SLT and Dialog connections, but were accessible outside the country. Separately, the government continues to block some pornographic sites. The government blocked social media and communication platforms three times in April and May 2019, in the aftermath of the Easter Sunday suicide bomb attacks, and once for over a week in March 2018 in response to violence in Kandy (see A3). Authorities claimed the restrictions were necessary to stop the spread of disinformation and hateful content, as well as limit sectarian violence during the politically tense weeks and months following the attacks. ⁴ The restrictions, however, prevented access to independent news sources and limited users’ ability to contact those in areas affected by the crisis. ⁵

B2 0-4 pts

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

3 / 4

Digital platforms, publishers, and content hosts do not report many government requests to remove content.

Between July and December 2019, Facebook restricted 847 pieces of content, of which 800 were temporarily restricted to comply with local electoral regulations pertaining to a “blackout” period for campaigning ahead of the 2019 presidential polls. Fifteen items were permanently restricted after being reported by the TRC, the Computer Emergency Readiness Team, or the Elections Commission. There were also restrictions for content that violated local laws on hate speech and extremism. Twitter reported no removal requests during the same time period. ¹ Also during the same time period, Google reported receiving one removal request related to defamation affecting eight items of content. ²

There have been increasing efforts from domestic actors—including government officials, civil society, and fact checkers—to work with international tech companies. For example, in March 2020, Facebook committed to remove false claims or conspiracy theories flagged by global and local health authorities related to COVID-19. ³ Also in March, it was reported that the Elections Commission would be working with officials from Facebook, Twitter, and YouTube who would be monitoring content during the upcoming August general elections to ensure the platforms would not be misused for content like hate speech. ⁴

Previously, during the 2019 presidential elections, Facebook also committed to removing content that would deter people from voting. ⁵ Separately, ahead of the vote, the Election Commission warned that it would take legal action against electronic and online media organizations spreading false content or hate speech. ⁶

Rights activists have expressed concerns about Facebook’s content moderation practices. For instance, critics have expressed concerns

about the impact of automated content review related to COVID-19 on Sinhala and Tamil content, ⁷ and pointed out that posts promoting misinformation on Facebook continued to be shared more than credible news, despite the platform pledging to remove some types of misleading content. ⁸ Previously, civil society organizations criticized a January 2019 meeting between senior Facebook employees and government officials including then-president Sirisena, former president Mahinda Rajapaksa, and then–prime minister Ranil Wickremesinghe. ⁹ The meeting was ostensibly about disinformation, although activists were concerned that the participants focused on content moderation and censorship.

Facebook’s content removal policies generated controversy in the aftermath of communal violence in March 2018, with Facebook being criticized for failing to remove hateful content in the Sinhala language that analysts argue has encouraged violence against Muslims. ¹⁰ In June 2018, Facebook representatives met with local civil society activists and made commitments to improve their language capabilities to better moderate content. ¹¹

After the presidential election, the Ministry of Defense announced that a new mechanism would be introduced to immediately remove social media posts that were defamatory or spread ethnic- or religious-based hatred. This new mechanism is expected to be part of the forthcoming National Cyber Security Strategy, which had not yet been introduced as of July 2020 (see C2). ¹²

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	2 / 4
---	---------------------

There is a lack of transparency around restrictions of online content, but a 2017 right to information (RTI) request revealed some of the government’s blocking procedures. Following the Easter Sunday attacks,

the government claimed it would introduce new social media regulations, but no concrete legislation had been proposed as of February 2020. ¹

The blocking of Lankaenews prompted three civil society organizations to file an RTI request about the government's blocking procedures in 2017 (see B1). ² The government's response revealed that blocking orders can originate from the Ministry of Mass Media and the Presidential Secretariat for a number of reasons, including "publishing false information" and "damaging the president's reputation." ³ Orders are then sent to the TRC, which instructs ISPs to block the content. The TRC denied part of the RTI request on national security grounds, and an appeal of the case was heard before the RTI Commission in the spring of 2018. ⁴

There is no record of ISPs challenging the TRC's blocking orders at the commission itself or through the courts. It is not clear if the TRC can impose financial or legal penalties on telecommunications companies that do not comply with blocking orders since the conditions of such orders are unknown to the public. Under the Telecommunications Act, ISPs are licensed by the Ministry of Telecommunications, but the TRC can make recommendations on whether or not a license should be granted. The ministry can impose conditions on a license, requiring the provider to address any matter considered "requisite or expedient to achieving" TRC objectives. ⁵

There is no independent body regulating content, which leaves limited avenues for appeal (see A5). Content providers have filed fundamental rights applications with the Supreme Court to challenge blocking orders, ⁶ but under former president Mahinda Rajapaksa, the lack of public trust in the politicized judiciary and fear of retaliatory measures presented significant obstacles for would-be petitioners. ⁷

In July 2018, Facebook unveiled a new misinformation policy for several countries, including Sri Lanka, which aims to proactively remove misleading content that could result in real-world harm. ⁸ However, civil society groups have concerns about the policy, arguing that it places too

much pressure on local organizations and not enough responsibility with the platform. ⁹

B4 0-4 pts

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

2 / 4

Following the November 2019 election of President Gotabaya Rajapaksa, journalists and activists reported an increase in self-censorship around political issues. In previous years, journalists have noted a tendency to self-censor when covering the president and the first family. ¹

Harassment and intimidation leveled against journalists may also contribute to self-censorship (see C7).

Gihan Nicholas—who works for the news website NewsHub, which had criticized the Rajapaksas ahead of the election—reported that after the vote, “The mood is one of self-censorship. [Journalists are] holding back.”

² Members of Tamil and Sinhala media outlets have reportedly faced increasing pressure from officials and report increasing self-censorship.

³ Journalists from the Tamil daily *Thinakkural* and the English-language *Daily Express* said they were hesitant to be critical of the Rajapaksas; *Thinakkural* journalists reportedly considered rights violations, the army, corruption, missing people, and land appropriation to be “sensitive” topics. The Committee to Protect Journalists also noted that at least two journalists went into exile following the presidential election. ⁴

Separately, a few prominent anonymous Twitter accounts sharing satirical or other forms of political speech, notably on Tamil issues or focused on the north of the country, closed their accounts due to security concerns.

⁵

Under former president Sirisena, self-censorship by journalists online appeared to be decreasing, in part due to the government’s stated commitment to press freedom. Both traditional and online media outlets expressed a diversity of political viewpoints, including criticism of the government.

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?

2 / 4

Score Change: The score declined from 3 to 2 after a new report identified Sri Lanka as having coordinated cybertroop teams that manipulate information across major social media platforms, as well as the continued proliferation of disinformation online.

The spread of disinformation and misinformation has been a growing concern in recent years. A report from the Oxford Internet Institute released in September 2019 identified Sri Lanka as having coordinated cybertroop teams that manipulate information on Facebook, Twitter, and YouTube on behalf of government agencies, politicians, and political parties. ¹ The report found evidence that Sri Lankan teams work to support preferred messaging, attack opposition, create divisions, and suppress critical content.

Disinformation increased in the lead-up to and during the November election period, including some originating from political parties and candidates. For example, a Facebook page associated with Gotabaya Rajapaksa incorrectly suggested that Muslim groups destroyed Buddhist statues at a heritage site. ²

Misinformation spread by ordinary users is a problem in Sri Lanka. For instance, false posts circulated online in March 2020 touting coronavirus cures and claiming that Sri Lanka had eradicated the virus. ³ Following the bombings on Easter Sunday, false or manipulated information was quickly shared online. ⁴ For example, rumors spread that the water supply in Hunupitiya was poisoned and a fake Facebook page masquerading as the police spread rumors that users could be arrested if they used VPNs. ⁵

Platforms such as Facebook have amplified and spread inflammatory speech. ⁶ Following communal riots in Ampara and Digana, Facebook's slow response to inflammatory online speech, such as content that

implored followers to “kill all Muslims, don’t even save an infant,” became an international concern. The platform has since introduced a new misinformation policy. ⁷

B6 0-3 pts

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

2 / 3

Some government regulations threaten the economic viability of online publishers and start-up platforms. ¹ In late 2019, the government issued new guidelines for media accreditation that include websites and online journalists covering news and current events. ² Beginning in 2020, a special committee appointed by the Director of Government Information is expected to issue media cards, and websites will be required to register with the Ministry of Mass Media and Information. ³ The purported purpose of the guidelines is to ensure better media practices.

The government also maintained news site registration requirements introduced by previous administrations. During Mahinda Rajapaksa’s presidency, the Ministry of Mass Media directed all news sites to register for a fee of 25,000 rupees (\$130), with an annual renewal fee of 10,000 rupees (\$54).

B7 0-4 pts

Does the online information landscape lack diversity?

3 / 4

Diverse content is generally available online. Social media and communication platforms and blogs are popular and widely available, diversifying the media landscape and spurring local debate. Diverse sources of information online in English, Sinhala, and Tamil are available, including on socioeconomic and political issues, despite a history of censorship and instances of intimidation targeting online journalists during the reporting period (see C7).

Sites such as Vikalpa Groundviews and Maatram *highlight* citizen-generated content that would otherwise be overlooked by mainstream media. ¹

Other curated websites contribute to this diversity. ReadMe offers news on technology and the start-up Roar reports on political, social, and economic issues. ² Manthri.lk is a nonprofit platform that monitors elected officials' participation and attendance, the diversity of issues they discuss, and their contributions to legislative functions. ³ Additionally, the online news magazine Counterpoint, which launched in February 2018, focuses on long-form journalism and investigative and political content. ⁴ The South Asian magazine of politics and culture *Himal Southasian* also launched a website and membership model in January 2020. ⁵

The Sinhala newspaper and website *Anidda*, which launched in April 2018, ⁶ was one of the few outlets to criticize the ruling party during that year's constitutional crisis. ⁷ There have been a number of new initiatives from civil society, such as the website the Divide, which examines the gaps between Sinhala- and Tamil-language newspapers in their reporting on gender, minority groups, transitional justice, and political reconciliation. ⁸

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	4 / 6
--	--------------

The web has provided an avenue for robust digital activism and engagement on political issues in Sri Lanka, although most campaigns register uneven progress in achieving their goals. Many are hitched to discrete events, crises, or stalled political processes, and campaigners are generally unable to gather the momentum needed to drive meaningful change and long-term citizen participation. However, blocks on social media platforms in 2018 and 2019 impacted citizens' ability to access news and information, albeit temporarily.

In the lead-up to and during the 2019 presidential election, people used the hashtags #PresPollSL and #PresPollLKA to discuss the vote and candidates online. Following the Easter Sunday attacks during the previous coverage period, users disseminated developments online through hashtags such as #EasterSundayAttacksLK.

Activists and civil society groups used the hashtag #DisappearedSL to draw attention to and track the protests by families of those who disappeared across the nation's north and east during the civil war. ¹ The hashtag #1000wagehike has been used to highlight wage negotiations for estate workers and the continued marginalization of those workers particularly among Malaiyagha Tamils. ² In 2020, on Independence Day, which falls on February 4, a group of activists gathered to sing the national anthem in Tamil since the Government decided not to allow the Tamil version to be sung at its official celebration for the first time since 2015. The video was shared on social media and received some pushback. ³

C. Violations of User Rights

During the coverage period, people were arrested for their online speech and held in short-term pretrial detention. Authorities also rolled out new surveillance efforts amid the COVID-19 pandemic. In the lead-up to, during, and following the presidential election, journalists working for online outlets faced intimidation, harassment, and at times physical violence.

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?	2 / 6
--	--------------

Score Change: The score improved from 1 to 2 after the government lifted the April 2019 state of emergency and associated emergency regulations that restricted free expression rights.

Although internet access is not guaranteed as a fundamental right in Sri Lanka's legislation, Article 14 (1)(a) of the constitution protects freedom of expression, subject to restrictions related to the protection of national security, public order, racial and religious harmony, and morality. There are no specific constitutional provisions guaranteeing freedom of expression online. During the previous coverage period, the government moved to restrict free expression and press freedom with the implementation of emergency regulations and the approval of new amendments targeting false information online (see C2).

Following the Easter Sunday attacks in April 2019, the government declared a state of emergency and passed emergency regulations. ¹ The regulations created a new competent authority appointed by the president. ² This authority could limit the publication of certain materials, including online materials, such as content deemed threatening to national security or disruptive to public order or the provision of essential services. The authority required that certain types of content be reviewed before being published. The regulations also prohibited the spread of false statements that could cause public disorder or alarm. Under the regulations, people could appeal decisions made by the competent authority to new advisory committees. The state of emergency was lifted in August 2019. ³

Since the passage of the Right to Information Act in 2017, ⁴ citizens have submitted thousands of RTI applications on issues ranging from legislation on the rights of people with disabilities to the blocking of websites (see B3). ⁵

A culture of impunity, circumvention of the judicial process through arbitrary action, and a lack of adequate protection for individuals and their privacy compounded the poor enforcement of freedom of expression guarantees under former president Mahinda Rajapaksa's government. These issues persisted into President Sirisena's government. ⁶

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?

1 / 4

Several vaguely defined, overly broad laws can be abused to prosecute users and restrict online expression. The 2019 emergency regulations also stipulated prison terms and fines for authors, editors, and publishers of some forms of online speech (see C1). ¹

In June 2019, the cabinet approved vague amendments to the Penal Code and Criminal Procedure Code that criminalize the spread of “false news” affecting “communal harmony” or “state security.” These terms are left undefined in the amendments, leaving them open to abuse. ² However, as of the end of the coverage period, the amendments had not been passed by Parliament.

The government is drafting a Cyber Security Act, which is expected to tackle cybercrime, the nonconsensual dissemination of intimate images, and hacking and intellectual property theft. ³ A proposed draft of the bill was posted online in May 2019. ⁴ The information technology (IT) industry criticized the lack of transparency in the process and the broad definitions contained in the draft bill. ⁵ Some civil society representatives also criticized the limited time for feedback and noted that Sinhala and Tamil translations were not available for consultations. ⁶ Others pointed out that broad definitions for terms like “critical information infrastructure” and “cyber security incidents” could allow for the extension of government control over private institutions, could extend criminality to “actions that are otherwise acceptable but politically inconvenient” and could have a chilling effect on privacy and freedom of expression. ⁷ The final act is not yet publicly available as of July 2020, and it is unclear how or if the proposed mechanism to remove content from social media will be worked into the final act (see B2).

Publishing official secrets, information about Parliament that may undermine its work, or “malicious” content that incites violence or disharmony can result in criminal charges. ⁸ Then–government information director general Sudarshana Gunawardana stated in March 2018 that incitement to violence, including on social media, is contrary to Article 28 of the constitution and Section 100 of the Penal Code, as well

as Section 3 of the International Covenant on Civil and Political Rights (ICCPR), to which Sri Lanka is a party. ⁹

In February 2020, Sri Lanka's Minister of Foreign Relations told the UN that it would review and amend the broad Prevention of Terrorism Act (PTA) 1979, rather than pass the draft Counter Terrorism Act proposed by the previous government. ¹⁰ The PTA has been previously used to crack down on critical online content, including speech from journalists. ¹¹

Authorities have increasingly manipulated the ICCPR Act 2007, which enshrines the ICCPR in Sri Lankan domestic law, to criminalize online speech (see C3). ¹² Section 3(1), for example, prohibits national, racial, and religious hatred if it incites discrimination, hostility, and violence. Those charged under the act can only be granted bail by a high court.

C3 0-6 pts

Are individuals penalized for online activities?	3 / 6
---	--------------

During the coverage period, a growing number of people were prosecuted in retaliation for their online activities, including criticism of the government.

In August 2019, the award-winning author and poet Shakthika Sathkumara was released on bail. ¹ In April 2019, he was arrested and charged under the ICCPR Act and Penal Code for a short story he shared on Facebook that reportedly alluded to same-sex sexual activity and child abuse within the Buddhist clergy. ² The Attorney General has yet to decide whether to file formal charges. In December 2019, a petition was filed with the UN Working Group on Arbitrary Detention, arguing that Sathkumara's prolonged detention and ongoing legal case violated the government's commitments under the ICCPR and the Universal Declaration of Human Rights. ³

Ramzy Razeek, a commentator who regularly used Facebook to discuss political and social topics such as ethnic harmony, the rights of marginalized communities, and gender, ⁴ was detained on April 9 over

allegations that he violated the ICCPR Act and the Cyber Crimes Legislation. He remained in detention as of May 28. ⁵ It is believed that the post that led to his arrest discussed discrimination and hateful content against the Muslim community and called for an ideological struggle using “the pen and keyboard as weapons.” Before his arrest, Razeek had reported online death threats due to the post and had announced that he would no longer post about politics or national issues out of concern for his children’s safety (see C7). He was granted bail and released from detention in September 2020, after the coverage period. ⁶

Several people were arrested for online speech amid the COVID-19 pandemic. During March and April 2020, at least 17 people were arrested for allegedly spreading misinformation about the virus, including across social media. ⁷ Police visited the home of one student activist after he questioned the government in a Facebook comment. ⁸

Authorities also increasingly summoned and questioned journalists and others working for online news outlets over the coverage period (see C7). The Criminal Investigation Department questioned a reporter from TheLeader.lk and another from Voicetube.lk for several hours in late November. ⁹

During the previous coverage period, people were detained and released on bail after criticizing police on social media. For example, two men were charged in January 2019 with damaging public property and humiliating the police for posting a video on Facebook of themselves pretending to bribe a cardboard cutout of a traffic police officer. They were later released on bail. ¹⁰

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?

2 / 4

Users can freely use encryption tools, though there are some limits to anonymous digital communication. Real-name registration is required for mobile phone users under a 2008 Ministry of Defense program to curb

“negative incidents.” The program was bolstered in 2010 after service providers failed to ensure that subscribers registered. ¹ Access to public Wi-Fi hotspots requires a citizen’s national identity card number, ² which could be used to track online activity.

News sites are required to register under a procedure that lacks a legal foundation, according to critics (see B6). The registration form issued by the Ministry of Mass Media requires users to enter their personal details along with the name of the server, internet protocol (IP) address, and location from which content is uploaded. ³ The form does not refer to a law or indicate the penalty for noncompliance. Civil society groups fear the requirement could be used to hold registered site owners responsible for content posted by users or to prevent government critics from writing anonymously. ⁴

C5 0-6 pts

Does state surveillance of internet activities infringe on users’ right to privacy?

2 / 6

State surveillance of online activities undermines users’ right to privacy. The National Action Plan for the Protection and Promotion of Human Rights 2017–2021 contains the objective of ensuring the constitutional recognition of the right to privacy, but in practice, this right is frequently not respected. ¹

In an interview in April 2020, Sri Lanka’s Defence Secretary said that military intelligence was receiving cell phone contacts of patients from service providers. He said that the information was an important national security tool, as it was being used to track down those who had close contact with people who had tested positive for coronavirus or who were evading quarantine. ²

Following the Easter Sunday attacks, the government indicated its intention to ramp up monitoring and surveillance. In May 2019, the prime minister announced a plan to implement a Centralized and Integrated Population Information System (CIPIS) to track individuals engaged in

terrorism, money laundering, and transaction and financial crimes. ³ In August 2019, police announced that they were creating an integrated database and facial recognition system to “identify criminals” with Sri Lanka Telecom and other parties. ⁴

During a visit to China in May 2019, then-president Sirisena asked Chinese president Xi Jinping to share surveillance technology with Sri Lanka, citing the challenges of surveilling encrypted platforms. President Xi reportedly agreed to meet Sirisena’s request. ⁵ There has been no update on the outcome of this meeting.

The introduction of the electronic identity card (e-NIC) project has also raised surveillance concerns. The project includes a central database storing wide-ranging information and biometrics with “family tree” data. ⁶ Activists warn that this data could be used to target political opponents and is vulnerable to hacking. ⁷ President Rajapaksa has asked that the project be expedited. ⁸ There was little opposition to the project when it was first introduced, presumably because the government justified it as a needed improvement to government service delivery operations.

Extrajudicial surveillance of personal communications is prohibited under the Telecommunications Act No. 27 of 1996. However, communications can be intercepted on the order of a minister or a court, or in connection with the investigation of a crime.

The use of mobile apps and tracking tools amid COVID-19 raised privacy concerns (see C6). ⁹ The government-developed app Rakemu Api, which allows users to report their health status if they have come into contact with a COVID-19 patient or returned from overseas in the past two weeks. There was a lack of transparency about who has access to the data collected by the app, how the data can be used, how the information is stored, and for how long. ¹⁰

State agencies reportedly possess some technologies that could facilitate surveillance. In March 2019, President Sirisena requested approval for the government to purchase \$38.9 million (7.11 trillion rupees) worth of surveillance technology from an unnamed Israeli company. Bypassing the normal procedures for purchasing such technology, Sirisena claimed the

request—which was purportedly related to tackling drug trafficking—was urgent and must be kept secret. ¹¹

In 2015, leaked documents indicated that the Milan-based firm HackingTeam was approached by several state security agencies seeking to acquire the company’s digital surveillance technologies. ¹² The leaks revealed that in 2014, the Ministry of Defense was planning to develop an electronic surveillance and tracking system with the help of a local university. ¹³ While no purchases of HackingTeam’s equipment were confirmed in the leaked documents, the papers did include a 2013 email exchange between a HackingTeam employee and an individual claiming to represent Sri Lankan intelligence agencies, which described confidential acquisitions of “interception technologies” the individual had brokered in the past. ¹⁴ Digital activists in Sri Lanka believe that the Chinese companies ZTE and Huawei, which collaborated with Mahinda Rajapaksa’s government in the development and maintenance of Sri Lanka’s ICT infrastructure, may have inserted backdoor espionage and surveillance capabilities into the technology. ¹⁵

C6 0-6 pts

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

3 / 6

There are some legal requirements for telecommunications companies to aid the government in monitoring users, and companies have reportedly provided data to authorities. A draft of a data protection law was completed during the coverage period, although a final draft is not yet public. ¹ Some feedback on the initial draft noted that it was modeled on the European Union General Data Protection Regulation. ²

Amid COVID-19, the country has integrated its defense apparatus into its pandemic response. Military Intelligence has obtained personal data from mobile service providers to identify people who have interacted with confirmed patients or evaded quarantines. ³

In 2013, Dialog CEO Hans Wijesuriya denied the existence of a comprehensive surveillance apparatus in Sri Lanka but agreed that telecommunications companies “have to be compliant with requests from the government.” ⁴ In 2016, however, SLT engineers apparently defied orders from their superiors to install equipment purchased for surveillance. ⁵ The nature and number of government requests for data is unknown, since there is no legal provision that requires officials to notify the targets. Some companies disclose information; from July to December 2019, Facebook reported receiving 44 requests and providing data in response to 32 percent of the requests. ⁶ Twitter reported six requests from the government for user data during the same time. ⁷

In January 2018, SLT opened a Tier 3 National Data Center, ⁸ which hosts local data and serves as a cloud computing service, although the country does not mandate data localization. ⁹

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?	3 / 5
--	--------------

More cases of intimidation against both journalists and ordinary users were reported during the coverage period, notably increasing in the lead-up to, during, and after the November presidential election.

In November 2019, police raided the office of news website newshub.lk using a search warrant that had expired 11 months prior. The police searched computers, servers, and laptops, reportedly seeking material that mentioned “gota,” a seeming reference to President Gotabaya Rajapaksa. ¹ Journalists with online news sites theleader.lk and VoiceTube were also summoned and questioned at length by the Criminal Investigation Department (CID) (see C3). The editor of the Tamil newspaper *Thinappuyal*, a print outlet with an online version, was questioned by the police in Vavuniya. In December, the former head of the state-run Associated Newspapers of Ceylon’s new media division, which manages the outlet’s online and social media presence, was

assaulted by a group of individuals with ties to the ruling political party.² In January 2020, a group of Tamil journalists in Batticaloa, some of whom worked for online outlets such as Lankasri, received death threats and accusations that they had received money from members of the Liberation Tigers of Tamil Eelam rebel group living abroad.³ Groups of men had also attacked journalists from the *Daily Mirror/Lankadeepa* and *Resa* newspapers, although it is unclear whether the attack was linked to online activity.⁴

Intimidation and harassment also increased around the COVID-19 pandemic. For example, police visited the home of a student activist after he criticized the government on Facebook (see C3).⁵ Separately, when calls to boycott Muslim businesses and allegations that Muslims were spreading COVID-19 were disseminated on social media, they were not refuted by the government. Senior government officials also implied that the virus was rife among the Muslim community in Sri Lanka, drawing condemnation from civil society.⁶

During the previous regime, journalists were also the targets of assault, intimidation, and harassment. In May 2019, Kanapathipillai Kumanan, a freelance correspondent with the Tamil Guardian news site and the *Virakesari* newspaper, was assaulted by a police officer.⁷

Families of journalists have been targeted for online harassment. In June 2018, Sandya Eknaligoda, wife of disappeared journalist Prageeth Eknaligoda, filed a complaint with the CID about a slew of social media posts containing hateful content about her and her family.⁸

Women have been subjected to misogynistic and intrusive posts on social media, especially on Facebook. For example, intimate images have been shared in Facebook groups without the subjects' consent, often with abusive or derogatory captions.⁹ Female activists and politicians have also endured threats and intimidation online that have affected their work.¹⁰ Two Tamil women who were planning to contest the August 2020 parliamentary election were viciously attacked online.¹¹ Members of the LGBT+ community were also the target of hate speech, and were "outed" online.

A February 2018 report from the Sri Lanka Campaign for Peace and Justice included interviews with 27 individuals in the north who detailed ongoing surveillance, harassment, and intimidation by an array of state security agencies, including through phone calls and text messages. ¹² The report noted that among those targeted were human rights activists, survivors of the civil war, and members of the broader public.

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	2 / 3
--	--------------

Although government and business websites are vulnerable to hacking and other cyberattacks, the problem is not widespread in Sri Lanka. Cyberattacks occasionally targeted government critics, such as the TamilNet news site, under former president Mahinda Rajapaksa. ¹

On May 18, 2020, recognized as the anniversary of the end of Sri Lanka's civil war, several websites were hacked by a group calling itself Tamil Eelam Cyber Force. Several institutions, including a media organization, a diplomatic mission, and other private and state organizations, were affected. ² At the end of May, the same group defaced government websites, including the websites of the Sri Lankan Bureau of Foreign Employment; the Ministry of Public Administration, Home Affairs, Provincial Councils and Local Government; and, briefly, the Ministry of Health. ³

In June 2020, after the coverage period, several journalists' WhatsApp accounts were targeted by SIM-swapping attacks, which occur when a hacker convinces a service provider to switch a phone number to a new device that is under their control. ⁴ This allows the hacker to access the targeted person's two-factor authentication. Those affected included members of the GroundViews WhatsApp group, which were subsequently shut down, and potentially other journalist WhatsApp groups as well.

The draft Cyber Security Act, which would establish the Cyber Security Agency and implement the National Cyber Security Strategy of Sri Lanka,

is expected to include provisions for protection against hacking (see B2 and C2). ⁵

Hackers frequently attack government and business websites, and in 2016 one technology company placed Sri Lanka among the top 10 countries in the Asia-Pacific region facing increased threats to cybersecurity. ⁶ In May 2019, several local websites, such as that of the Kuwaiti embassy in Colombo, were defaced by unknown hackers. ⁷



On Sri Lanka

See all data, scores & information on this country or territory.

[See More](#) >

Country Facts

Global Freedom Score

55/100 Partly Free

Internet Freedom Score

52/100 Partly Free

Freedom in the World Status

Partly Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested
Yes

In Other Reports

[Freedom in the World 2020](#)

Other Years

2019

**Be the first
to know
what's
happening.**

Email

Join the Freedom
House monthly
newsletter

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