

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	655
Land:	Sri Lanka
Kilde:	Freedom House
Titel:	Freedom on the Net 2021 - Sri Lanka
Udgivet:	21. september 2021
Optaget på baggrundsmaterialet:	13. januar 2022

Sri Lanka

PARTLY FREE

51
/100

A. <u>Obstacles to Access</u>	11 / ₂₅
B. <u>Limits on Content</u>	23 / ₃₅
C. <u>Violations of User Rights</u>	17 / ₄₀

LAST YEAR'S SCORE & STATUS

52/100 **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 and 2021, which enabled Sri Lankans to engage in digital activism around a broad range of issues, the online space for free expression continued to shrink. Journalists and activists reported increased intimidation and harassment, contributing to self-censorship and a more fearful climate. Separately, arrests for online activity related to COVID-19 and environmental issues increased and the police arrested a few individuals without a warrant for their online speech. An online news site became the target of distributed-denial-of-service (DDoS) attacks, while government websites, including the prime minister's website, were hacked.

Sri Lanka 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. However, the Sirisena administration was slow to implement transitional justice mechanisms needed to address the aftermath of a 26-year civil war between government forces and ethnic Tamil rebels, who were defeated in 2009. Gotabaya Rajapaksa's election as president in November 2019 and the Sri Lanka Podujana Peramuna's victory in the August 2020 parliamentary polls have emboldened the Rajapaksa family, which has taken steps to empower the executive and roll back accountability mechanisms for civil war-era rights violations.

Key Developments, June 1, 2020 – May 31, 2021

- There were no reported blocks or restrictions on internet during the coverage period, allowing Sri Lankan users to increasingly mobilize around a range of issues online (see B8).
- Law enforcement officials increasingly arrested individuals for online posts related to COVID-19, environmental issues, and racial relations in Sri Lanka. The police arrested several individuals without a warrant for their online posts (see C3).
- The state-owned Sri Lanka Telecom (SLT) introduced unlimited data packages which blocked virtual private networks (VPNs), torrents, peer-to-peer (P2P) applications, and messaging app Telegram as part of their terms and conditions (see C4).

- Amid the COVID-19 pandemic, government initiatives for contact tracing and quarantine compliance—including a new smartphone app and the retrieval of personal data from mobile service providers by military intelligence—raised privacy and surveillance concerns (see C5 and C6).
- Government and media organizations continue to be targeted by cyberattacks and hacked. An online news site, Colombo Gazette, was the target of a DDoS attack (see C8).

A. Obstacles to Access

A1 0-6 pts

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

3/6

Score Change: This score declined from 4 to 3 to correct for a methodology error in one of the sources used to calculate internet penetration rates. This score change does not necessarily reflect a change in infrastructural limits to internet access, speed, or quality.

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. According to the Telecommunications Regulatory Commission of Sri Lanka (TRCSL), there were over 17.2 million mobile broadband subscriptions as of March 2021. ¹ In the same month, there were over 2.1 million fixed-line broadband subscriptions.

The government is interested in expanding internet access and digital infrastructure projects. In a manifesto, President Gotabaya Rajapaksa laid out plans to make Sri Lanka “digitally inclusive” by 2024; 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 (ICTA) is also focused on improving and lowering the cost of access to the internet and other digital services (see A2). ³

Private companies are also working to expand service. In 2019, internet service providers (ISP) Dialog Axiata had over 2,500 pay-to-use Wi-Fi hotspots around the country. ⁴ In July 2020, Dialog invited customers to register devices and use its 5G trial network. ⁵ As of July 2020, Dialog equipped 20 percent of its base stations with 5G technology. In May 2021, SLT announced that it was executing its plan to provide fiber-optic connections nationwide. ⁶ In July 2020, SLT also announced plans to deploy a fiber-to-home network using Nokia-sourced technology, allowing high-speed services for 200,000 enterprise and residential users. ⁷ Ratings agency Fitch Ratings, however, predicted that SLT's 5G rollout would be delayed past 2022. ⁸ Hutch, another ISP, successfully rolled out 4G nationwide during 2020. ⁹

A2 0-3 pts

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

1/3

Mobile internet connectivity is affordable, although gender-based and urban-rural digital divides persist. In a 2019 survey, 25 percent of respondents said cost of data was a limiting factor in internet use. According to cable.co.uk's 2020 study of global internet prices, Sri Lanka's average monthly price for fixed-line broadband was 1,872 rupees (\$9.58). For comparison, mean household income in Sri Lanka was 62,237 rupees (\$341) according to the 2016 Household Income and Expenditure Survey. ¹⁰ Prices for mobile broadband vary, and Sri Lanka has the 7th cheapest data-only mobile broadband plans in the world. ¹¹ According to the International Telecommunication Union (ITU), the cost of high-consumption mobile-data and voice basket packages amounted to less than 1 percent of the country's gross national income (GNI). ¹²

Urban residents benefit from infrastructural advantages, are better connected to the internet, and are considered relatively more "computer literate." The province with the highest percentage of households accessing the internet is the Western Province, the country's most populous, ¹³ where Colombo and other urban areas boast well-developed infrastructure. Government statistics for 2020 found about 45.2 percent of Western Province residents to be "computer literate," ¹⁴ a category that excludes those whose only digital literacy is through smartphones or tablets. By comparison, the national digital literacy rate, which includes those able to use any digital device, is

50.1 percent compared to a national computer literacy rate of 32.3 percent— showing the shift away from personal computers. ¹⁵

The civil war, which ended in 2009, delayed infrastructure development in the Northern and Eastern Provinces. However, the telecommunications infrastructure in these provinces has improved in recent years, leading to steady growth in internet usage. In 2020, 18 percent of Northern Province residents were categorized as computer literate. ¹⁶ Compared to urban areas, rural and up-country Tamil communities have significantly lower computer and digital literacy rates. ¹⁷

Schools with digital facilities often lack corresponding digital literacy programs. 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. ¹⁸ In February 2021, the Education Ministry’s information technology (IT) director warned only 30 percent of the student population had access to, or could afford, online learning, affecting students who had to adjust to remote learning during COVID-19. The government, however, also broadcasts lessons on television and radio. ¹⁹ During the pandemic, some children struggled with poor mobile signals while trying to attend online classes.

For a number of years, the ICTA has promoted digital literacy in rural areas by establishing community-based e-libraries and e-learning centers, ²⁰ though some local journalists have criticized aspects of the initiative. ²¹ In 2017, the Education Ministry inaugurated the country’s first “cloud smart classroom,” a pilot project for digital interactive learning. ²² Those who participated in the cloud smart classroom reported higher attendance rates and performance. ²³ In February 2021, a US-funded “smart classroom” was opened in the northern city of Vavuniya. ²⁴

A3 0-6 pts

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

4/6

The government refrained from restricting connectivity and blocking social media platforms during the coverage period. However, the government has blocked social media platforms in the past.

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. ²⁵ For nine days directly following the attacks, Facebook, WhatsApp, YouTube, Instagram, Snapchat, and Viber were all blocked, as was at least one popular VPN. ²⁶

The government had previously restricted connectivity in the Kandy district following communal violence in March 2018. In response to the violence, the Defense Ministry ordered a nationwide block of Facebook, WhatsApp, Instagram, and Viber. ²⁷

Sri Lanka has access to multiple international cables, but most of the landing stations for these cables are controlled by the majority state-owned SLT, giving the government control over internet infrastructure. ²⁸ SLT's capital expenditure was disrupted in 2020 due to COVID-19, but the company is expected to invest in fiber-optic infrastructure in 2021. ²⁹ The company is reportedly planning to invest \$60 million in the new SEA-ME-WE submarine cable running from Singapore to France. ³⁰ 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 for the project. The cable, built by Huawei Marine Networks, was ready for service in February 2021. ³¹

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 besides SLT in Sri Lanka. ³² SLT remains a key player in the information and communication technologies (ICT) market, and the firm imposes price barriers by forcing competing service providers to lease connectivity from SLT, which charges high rates. ³³

Dialog Axiata remains the largest mobile service provider, with over 16.9 million subscribers as of June 2021. ³⁴ SLT Telecom and Mobitel, a mobile service provider and subsidiary of SLT, reorganized their operations under the SLT-Mobitel brand in

January 2021. **35** Mobitel is the second largest mobile service provider, with over 7.9 million subscribers at the end of 2020. **36** Hutch had the third largest number of subscribers, with over 5.3 million reported in July 2019. In 2020, Hutch reported a 7 percent decrease in active customer accounts. **37** Airtel had 2.87 million subscribers in 2021. **38**

The TRCSL, in April 2021, announced plans to introduce number portability by the end of the year. Number portability will allow customers to change their service providers to get better or more affordable services without changing their phone number. The TRCSL noted that number portability will push ISPs to provide better service in order to retain customers. **39**

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. **40** In August 2018, the government removed telecommunications floor rates for call charges in hopes of increasing competition among service providers. **41**

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, in which Dialog accused SLT of violating intellectual property rights. **42**

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

In November 2020, the TRCSL, the ICTA, and several other bodies were brought under the Technology Ministry, which is directly under presidential purview. Previously, in

December 2019, President Rajapaksa issued a gazette notification that the TRCSL would be brought under the purview of the Defense Ministry, a reorganization that heightened concerns about the TRCSL's independence and about potential government surveillance projects. ⁴³ As the TRCSL remains under presidential purview through the Technology Ministry, there are continued concerns about the regulatory body's independence. ⁴⁴

The TRCSL 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. ⁴⁵ Analysts have asserted that spectrum allocation and refarming—the more efficient reallocation of spectrum—have been administered in an ad hoc manner, but procedural transparency has improved over time. ⁴⁶ However, regulatory reforms to improve the TRCSL's performance and increase its independence are still necessary.

Under former president Mahinda Rajapaksa, many of the TRCSL's interventions to restrict online content and pronouncements on strengthening internet regulations were partisan and extralegal. ⁴⁷ In 2017, the Colombo High Court found former TRCSL chairperson Anusha Palpita and former presidential secretary Lalitha Weeratunga guilty of misappropriating TRCSL funds for Rajapaksa's presidential campaign. They received three-year prison sentences and fines that year. In November 2020, however, they were acquitted on appeal. ⁴⁸ In the interim, a travel ban imposed against Weeratunga was temporarily lifted to allow him to travel to India along with Rajapaksa. ⁴⁹

Successive regimes have largely chosen political allies to head the TRCSL. The current acting chairman is Jayantha de Silva, secretary to the Technology Ministry. The current director general, Oshada Senanayake, was appointed in November 2019 and is the former head of a software company; ⁵⁰ Senanayake publicly advocated for a Gotabaya Rajapaksa presidency when speaking to a convention of academics and professionals. ⁵¹ In December 2019, secretary to the Defense Ministry, and former military officer Kamal Gunaratne, was appointed chairman of the TRCSL, demonstrating another example of the president giving the post to political and military associates.

B. Limits on Content

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?

4/6

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.

SLT's unlimited data packages, which became available in April 2021, blocks torrents, P2P applications, and Telegram under their terms and conditions (see C4).

Lankaenews remained blocked on Dialog connections during the coverage period, although it was accessible on SLT connections. The website was reportedly first blocked for publishing stories critical of then president Sirisena. **52**

During the coverage period, tests from the internet censorship organization OONI revealed signs of HTTP blocking for several websites. Sankanthi24.com, a Tamil news site, first showed signs of being blocked in June 2020 and continued to show signs as of June 2021 on Dialog and SLT connections, though it was accessible outside the country. **53** Adult dating site adultfriendfinder.com also showed signs of HTTP blocking on Dialog connections starting from September 2020 to June 2021, though it was accessible on SLT. **54** The official website of the US Navy's Sea, Air, and Land (SEAL) teams showed signs of TCP/IP blocking from June 2020 to June 2021 on both Dialog and SLT connections, but remained accessible outside the country. **55** US-based news site Jezebel appeared to have been affected by domain name system (DNS) tampering on Dialog connections from September 2020 to June 2021. **56**

Separately, the government has blocked websites that address health and intimate issues. Teen health, relationship, and sexuality site teenhealthfx.com, which showed signs of DNS tampering in the previous coverage period, is now accessible on both Dialog and SLT connections. The government previously blocked social media and communication platforms three times in April and May 2019, in the aftermath of the Easter Sunday 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. ⁵⁷ The restrictions, however, prevented access to independent news sources and limited users' ability to contact those in areas affected by the crisis. ⁵⁸

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, particularly material that is protected by international human rights standards?

3/4

In recent years, the Sri Lankan government has considered instituting a legal framework to curb online speech it considers discriminatory along with speech it considers misleading. The government also issued takedown requests during the reporting period.

Between July and December 2020, Facebook temporarily restricted access to 1,643 items to adhere to election guidelines related to that August's parliamentary polls. Election guidelines restrict candidates and supporters from campaigning in the two days before polling. Facebook also restricted access to one piece of content for violating privacy laws. ⁵⁹ In the same period, Google received 39 removal requests, including 9 requests over accusations of defamation, 8 over privacy or security concerns, 7 over nudity or adult content, 3 over harassment, 3 involving criticism of the government, and 3 involving religious content. Google also received 1 request each in categories of copyright, electoral, hate speech, impersonation, violence, and "other." One request came from the Criminal Investigations Department (CID) about two Blogger posts that were allegedly defaming a business. Google, however, did not comply with this request. ⁶⁰ Twitter reported one legal demand to remove content between January and June 2020, to which it did not comply.

After the presidential election in November 2019, the Defense Ministry announced that a new mechanism would be introduced to immediately remove social media posts that were defamatory or spread ethnic- or religious-based hatred. In November 2020, the government again announced its intention to introduce a regulatory framework based on Singapore's Protection from Online Falsehoods and Manipulation Act, aimed at curbing hate speech and misinformation. ⁶¹ In April 2021, the cabinet was granted approval to draft laws to curb false and misleading online

posts. ⁶² In December 2020, the government announced its intention to register foreign digital operators, although there have been no further updates on this effort.

63

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.

⁶⁴ The government's response revealed that blocking orders can originate from the Mass Media Ministry and the Presidential Secretariat for a number of reasons, including "publishing false information" and "damaging the president's reputation." ⁶⁵ Orders are then sent to the TRCSL, which instructs ISPs to block the content. The TRCSL 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. ⁶⁶ There are no records of ISPs challenging the TRCSL's blocking orders at the commission itself or through the court.

It is not clear if the TRCSL 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 Telecommunications Ministry, but the TRCSL can make recommendations on whether 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" TRCSL objectives. ⁶⁷

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, ⁶⁸ 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. ⁶⁹

Following the Easter Sunday attacks, the government claimed it would introduce new social media regulations. In December 2020, the government further explained it was

considering introducing registration requirements for foreign digital operators. No concrete legislation, however, had been passed as of June 2021. **70**

There have been increasing efforts from domestic actors—including government officials, civil society, and fact checkers—to work with international technology companies. For example, in March 2020, Facebook committed to removing false claims or conspiracy theories flagged by global and local health authorities related to COVID-19. **71** Also in March, it was reported that the Elections Commission (EC) would be working with officials from Facebook, Twitter, and YouTube to monitor content during the August polls and to ensure the platforms would not be misused for content like hate speech. **72** A report from youth group Hashtag Generation noted that Facebook did remove several instances of election-related hate speech, false news, and targeted harassment reported to them by the EC during the elections.

73

Previously, during the 2019 presidential elections, Facebook committed to removing content that would deter people from voting. **74** Separately, ahead of the vote, the EC warned that it would take legal action against electronic and online media organizations spreading false content or hate speech. **75**

Facebook's content-removal policies generated controversy in the aftermath of communal violence in March 2018. Facebook was criticized for failing to remove hateful Sinhala-language content that analysts argued encouraged anti-Muslim violence. **76** In June 2018, Facebook representatives met with local civil society activists and committed to improve their language capabilities to better moderate content. **77** In March 2020, critics pointed out that, as moderators transitioned to working from home, posts promoting misinformation on Facebook continued to be shared more than credible news, despite the platform pledging to remove some types of misleading content. **78** In May 2020, Facebook apologized for its role in the communal violence targeting Muslims in 2018, and released a human rights impact assessment report, which highlighted that the automated detection of hate speech in Sinhala and reporting channels within Facebook Messenger had been improved with added policy and language expertise. **79** The report made several recommendations on accountability, changes to platform architecture and grievance mechanisms, and improving community standards. Some recommendations drew mixed reactions from members of civil society, who noted shortfalls in terms of guidance in local languages for Sri Lankan users. **80**

Civil society organizations previously 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. ⁸¹ The meeting was ostensibly about disinformation, although activists were concerned that the participants focused on content moderation and censorship.

B4 0-4 pts

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

2/4

While self-censorship by journalists declined under the former Sirisena administration, journalists have since proceeded with caution when reporting on subjects that are considered sensitive.

In February 2021, UN High Commissioner for Human Rights Michelle Bachelet raised concerns that the surveillance and harassment reported by over 40 civil society organizations was having a “chilling [effect on] civic and democratic space and leading to self-censorship.” ⁸² 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. ⁸³ Harassment and intimidation leveled against journalists may also contribute to self-censorship (see C7).

Gihan Nicholas—who works for the news site 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.” ⁸⁴ Members of Tamil and Sinhala media outlets have reportedly faced increasing pressure from officials and are increasingly self-censoring. ⁸⁵ Journalists from the Tamil daily *Thinakkural* and the English-language *Daily Express* said they were hesitant to criticize 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 (CPJ) also noted that at least two journalists went into exile following the presidential election. ⁸⁶ 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. ⁸⁷

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

The spread of disinformation and misinformation has been a growing concern in recent years. A 2020 report from the Oxford Internet Institute identified Sri Lanka as having permanent cybertroop teams that manipulated information on Facebook, Twitter, and YouTube on behalf of politicians and political parties. ⁸⁸ The report found evidence that Sri Lankan teams work to support preferred messaging, attack the opposition, create division, and suppress critical content.

Disinformation increased in the lead-up to and during the August 2020 elections, including some originating from political parties and candidates. For example, one candidate implied that the elections commissioner was attempting to limit voter turnout in an interview shared on Facebook. Several political candidates also questioned the integrity of the vote-counting process on social media. ⁸⁹

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. ⁹⁰ In late 2019, the government issued new guidelines for media accreditation that include websites and online journalists covering news and current events. ⁹¹ Beginning in 2020, a special committee appointed by the director general of government information would issue media cards, and websites were

required to register with the Mass Media Ministry. ⁹² Websites that have not registered do not receive media accreditation, which restricts them from covering certain events and hinders their field reporting. 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 Mass Media Ministry directed all news sites to register for a fee of 25,000 rupees (\$130), with an annual renewal fee of 10,000 rupees (\$53).

B7 0-4 pts

Does the online information landscape lack diversity and reliability?

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).

Sri Lankans rely on several online outlets or companion websites for news and information, which are local and regional in scope. Roar Media reports on political, social, and economic issues. ⁹³ Sites such as Groundviews, Vikalpa, and Maatram highlight citizen-generated content. ⁹⁴ The nonprofit manthri.lk monitors elected officials' participation and attendance, the diversity of issues they discuss, and their contributions to legislative functions. ⁹⁵ Additionally, the online news magazine Counterpoint, which launched in February 2018, focuses on long-form journalism and investigative and political content. ⁹⁶ South Asian political and cultural magazine *Himal Southasian* launched a website and membership model in January 2020. ⁹⁷ The Sinhala newspaper and website *Anidda*, which launched in April 2018, ⁹⁸ was one of the few outlets to criticize the ruling party during that year's constitutional crisis. ⁹⁹ There have been a number of new initiatives from nonprofits, such as Divide, which examines the gaps between Sinhala- and Tamil-language newspapers in their reporting on gender, minority groups, transitional justice, and political reconciliation,

100 Minor Matters, a website dedicated to upholding the freedom of religion and belief. **101**

Some news sources became unavailable to Sri Lankan users during the coverage period. The British Broadcasting Corporation (BBC) announced the shutdown of Sinhala-language radio program *Sandeshaya* in December 2020, as part of its efforts to move BBC Sinhala online. As a result of this transition, individuals in rural communities without internet access will lose access to BBC content. **102** ReadMe, a site which offers news on technology and start-ups appeared to be inactive in May 2021.

Misinformation spread by ordinary users is a problem in Sri Lanka. For instance, false posts touting coronavirus cures and claiming that Sri Lanka had eradicated the virus circulated online in March 2020. **103** Once the country's vaccination program began, posts encouraging Sri Lankans to use herbal remedies instead of vaccines circulated online. These posts included misrepresented quotes of an opposition leader stating that the Oxford University–AstraZeneca vaccine was generally ineffective; he actually stated that the vaccines were ineffective only against new COVID-19 variants. **104** Following the 2019 Easter Sunday bombings, false and manipulated information was quickly shared online. **105** For example, rumors spread that the water supply in Hunupitiya was poisoned, while a fake Facebook page masquerading as the police spread rumors that users could be arrested if they used VPNs. **106**

Platforms such as Facebook have amplified and spread inflammatory speech. **107** 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 misinformation policy in July 2018 (see B3). **108**

B8 0-6 pts

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

5/6

Score Change: The score increased from 4 to 5 because there was a lack of internet shutdowns, social media blocks, or other internet restrictions, enabling Sri Lankan users to mobilize around a range of issues, during the coverage period.

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 online campaigns are prompted by 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.

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. Several hashtags were used for the August 2020 elections, including #GenElecSL, #GenElecSL2020, #LKA Elections2020 and #lkaParliament, as well as several hashtags in Sinhala and Tamil. ¹⁰⁹

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. ¹¹⁰ The hashtag #1000wagehike has been used to highlight wage negotiations for estate workers and the continued marginalization of those workers, particularly among Malaiyagha Tamils. ¹¹¹ The hashtag #StopForcedCremations was used by people to protest the government policy of cremating those who died due to COVID-19 without giving their families the option of burial. People used the hashtag and posted photos of white cloth online to show solidarity with offline protests. ¹¹² ¹¹³ Activists also used different hashtags, including #justiceforhejaaz and #FreeAhnaf, to highlight cases of detention under the controversial Prevention of Terrorism Act (PTA). ¹¹⁴ Women in media also shared experiences of sexual harassment at their workplaces using the #MeToo hashtag. ¹¹⁵

The government did not allow the Tamil-language version of the national anthem to be sung on February 4, 2020, when Sri Lanka celebrates its independence, marking the first time that version was banned since 2015. A group of activists gathered to sing the national anthem in Tamil. The video was shared on social media and received some pushback. ¹¹⁶

C. Violations of User Rights

Although internet access is not guaranteed as a fundamental right in 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. In 2019, 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).

In January 2021, the cabinet approved a proposal to amend the 1970s-era Press Council Law. The amendments would restructure the Press Council to regulate new outlets and electronic media as it already does in the print sector. ¹¹⁷ Civil society has expressed worries that the amendments would expand the government's control over online media and online speech. ¹¹⁸

Following the Easter Sunday attacks in April 2019, the government declared a state of emergency and passed emergency regulations. ¹¹⁹ The regulations created a new competent authority appointed by the president. ¹²⁰ This authority could limit the publication of certain materials, including online materials, which included 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. ¹²¹

Since the passage of the Right to Information Act in 2017, ¹²² 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). ¹²³

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 former president Sirisena's government and continue under the current administration. ¹²⁴

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?

1/4

Several vaguely defined, overly broad laws can be abused to prosecute users and restrict online expression.

In June 2019, the cabinet approved vague amendments to the criminal and penal codes 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. If passed, an offense can be punished with a fine of more than one million rupees (\$53,500), and a maximum prison sentence of five years. ¹²⁵ However, as of June 2021, the amendments have not been passed by Parliament. In April 2021, the government announced it was again considering penal-code amendments to criminalize false news, with news reports saying the government had approved concept papers in May 2021. ¹²⁶ The police recently cited a number of existing laws which could be used to arrest people for spreading misinformation, including sections of the penal code, the International Covenant on Civil and Political Rights (ICCPR) Act, the Computer Crime Act, the PTA, and sections of the Obscene Publications Act. ¹²⁷

The government has drafted a Cyber Security Act, which is expected to tackle cybercrime, the nonconsensual dissemination of intimate images, and hacking and intellectual property theft. ¹²⁸ A proposed draft of the bill was posted online in May 2019. ¹²⁹ The IT industry criticized the lack of transparency in the process and the broad definitions contained in the draft bill. ¹³⁰ Some civil society representatives also criticized the limited time for feedback and noted that Sinhala and Tamil translations were not available for consultations. ¹³¹ 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. ¹³² The final draft is

not yet publicly available as of June 2021, though it was reported that the bill would be finalized by the end of the year. ¹³³

Publishing official secrets, information about Parliament that may undermine its work, or “malicious” content that incites violence or disharmony can result in criminal charges. ¹³⁴ 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 ICCPR, to which Sri Lanka is a party. ¹³⁵

In February 2020, the foreign minister told the United Nations that the government would review and amend the PTA rather than pass the draft Counter Terrorism Act proposed by the previous government. ¹³⁶ The PTA has been previously used to crack down on critical online content, including speech from journalists. ¹³⁷ The government continues to use the PTA to detain writers, lawyers, and activists (see C3).

Authorities have increasingly manipulated the ICCPR Act, which enshrines the ICCPR in Sri Lankan domestic law, to criminalize online speech (see C3). ¹³⁸ 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, particularly those that are protected under international human rights standards?

3/6

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

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, ¹³⁹ was detained on April 2020 over allegations that he violated the ICCPR Act and the Cyber Crimes Legislation after he called for a campaign against Muslim discrimination using “the pen and keyboard as weapons.” Before his arrest, Razeek had reportedly received 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. He was granted bail and released from detention in September 2020. **140**

In January 2021, an activist and regular contributor to a news and opinions website was arrested under the ICCPR Act for a Facebook video in which he criticized a presidential statement and criticized monks using obscene language. **141** In August 2019, author and poet Shakthika Sathkumara was released on bail, after being detained for four months under the ICCPR Act and the penal code for a short story he shared on Facebook relating to the Buddhist clergy. **142** 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 Act and the Universal Declaration of Human Rights (UDHR). **143** He was discharged in February 2021, days before the UN Human Rights Council was due to meet. **144**

Authorities summoned and questioned journalists and others working for online news outlets (see C7). In August 2020, LankaNewsWeb editor Desmond Chathuranga de Alwis was arrested under the Computer Crime Act and Article 111 of the constitution for publishing reports in contempt of court and the judicial process; his computer and mobile phones were also confiscated. **145** He was granted bail in September 2020 but was ordered to report to the CID weekly and was barred from travelling overseas. **146**

In November 2020, a freelance journalist was arrested in secrecy in Batticaloa for posting photographs related to the LTTE; however, Reporters Without Borders received several reports that he had uploaded a note detailing events commemorating those who were killed during the country's civil war. **147**

Individuals faced detention for commenting on politicians or government affairs online during the coverage period. In June 2021, an individual was arrested without a warrant under Section 120 of the penal code and Computer Crime Act for sharing satirical posts about several politicians, including one accusing two state officials of bribing a Muslim to break two Buddhist statues. **148** The same day, the head of the Information Technology Society of Sri Lanka (ITSSL), Rajeev Yasiru Kuruwitage Mathew, was arrested without a warrant under the Computer Crime Act for spreading false information about a cyberattack on several government websites. He was remanded for two days before being released on bail. **149**

In May 2021, a Kotmale state officer was arrested for spreading false photographs related to deforestation; the CID said the officers' photographs actually showed a private land clearing. ¹⁵⁰ In June 2021, a Galle resident was arrested over a “defamatory” Facebook post referring to the sinking of a vessel and subsequent pollution but was bailed the same day. ¹⁵¹

Many young Tamils are being detained over their social media posts. ¹⁵² In March 2021, the Terrorism Investigations Department (TID) arrested two people in Jaffna for running a website and YouTube channel that allegedly promoted Liberation Tigers of Tamil Eelam (LTTE) propaganda. The TID also confiscated computers and other equipment belonging to the individuals. ¹⁵³ In February 2021, a Tamil youth was arrested by the TID under the PTA for TikTok posts featuring the LTTE.

Individuals also faced detention for posts related to the Easter Sunday attacks as well as religious content. In April 2021, a 19-year-old from Gampola was arrested under the ICCPR, Section 120 of the penal code, and Section 98 of the Police Ordinance for spreading false news with the objective of creating racial disharmony. He had allegedly posted that the country should “get ready for another easter attack,” referencing the 2019 Easter Sunday bombings, in response to the government banning the burqa. ¹⁵⁴ That same month, the TID arrested two individuals for spreading Wahhabism and extremism via social media. The two had helped publish videos and photographs connected to the Easter Sunday attacks and used a WhatsApp group in Qatar to spread extremist ideology. ¹⁵⁵ In October 2020, a woman was arrested over a video she uploaded to Facebook which the CID said promoted hate between Buddhists and Catholics, specifically against the archbishop of Colombo. ¹⁵⁶

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. ¹⁵⁷ Police visited the home of one student activist after he questioned the government in a Facebook comment. ¹⁵⁸ In November 2020, one person was arrested for uploading posts that alleged people were dying from COVID-19 in the streets. The police said four more had been identified making similar posts and would be arrested, though there were no further updates on these cases. ¹⁵⁹

--	--

Users can freely use encryption tools, though there are some limits to anonymous digital communication. Legal-name registration is required for mobile phone users under a 2008 Defense Ministry program to curb “negative incidents.” The program was bolstered in 2010 after service providers failed to ensure that subscribers registered. ¹⁶⁰ In October 2020, the TRCSL required all mobile phones to be registered with them; they announced that SIM cards on newly purchased unregistered phones would not be activated after a certain date. The TRCSL allegedly instituted this requirement to stop refurbished mobile devices from flooding the market. ¹⁶¹ Access to public Wi-Fi hotspots requires a citizen’s national identity card number, ¹⁶² which could be used to track online activity.

Service providers restrict or limit user access to security tools or certain applications. In May 2021, Swiss cybersecurity and internet privacy provider GlobeX Data signed a distribution agreement with Dialog Axiata for secure email, voice, text, and video services. ¹⁶³ In April 2021, SLT introduced unlimited data packages. Most Sri Lankan broadband connections are throttled after a set amount of data is consumed, and customers have long called for ISPs to offer unlimited packages. However, all but two SLT plans blocked VPNs, torrents, P2P applications, and Telegram as part of their terms and conditions. ¹⁶⁴ Dialog also announced it would be offering unlimited data plans, which also restrict the speed of the Telegram app. ¹⁶⁵

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 Mass Media Ministry requires owners, administrators, and editors to enter their personal details, including addresses, along with the domain name, and internet protocol (IP) address of the website, with applications reviewed by a panel appointed by the ministry secretary. ¹⁶⁶ 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. ¹⁶⁷

C5 0-6 pts

State surveillance of online activities undermines users' right to privacy. The National Action Plan for the Protection and Promotion of Human Rights 2017–21 contains the objective of ensuring the constitutional recognition of the right to privacy, but in practice, this right is frequently not respected. ¹⁶⁸ In March 2021, an anonymous Twitter user wrote that the Defense Ministry had activated the Pegasus spyware suite with the cooperation of Dialog Axiata and Mobitel. An opposition parliamentarian also stated that the government had obtained Pegasus. Dialog, however, claimed the allegations were false. ¹⁶⁹

In May 2021, the Health Ministry and the ICTA announced the launch of a digital vaccination ID, which would allow people to schedule COVID-19 vaccination and appointments and receive internationally valid vaccination certificates. The sign-up process, which is not live as of June 2021, appears to ask for health data to receive appointments and digital IDs. ¹⁷⁰ In February 2021, the State Ministry of Primary Healthcare, Epidemics, and COVID Disease Control launched a website for individuals to register for the COVID-19 vaccination program. ¹⁷¹ The website collected personal details including names, addresses, mobile numbers, and email addresses as well as health data. The data privacy statement did not detail how collected data would be used. An estimated 50,000 people registered on the site as of February 2021; the site was subsequently taken down.

The use of mobile apps and tracking tools amid COVID-19 raised privacy concerns (see C6). ¹⁷² A government-developed app, Rakemu Api, 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 collected data, how data can be used, how information is stored, and how long information is stored. ¹⁷³ The ICTA-developed Stay Safe app also traces those who have tested positive for COVID-19 and close associates. Several restaurants and hotels now offer the option of logging into Stay Safe for contact-tracing purposes. ¹⁷⁴ In an April 2020 interview, the defense minister disclosed that military intelligence was receiving mobile-phone contacts of patients from service providers. He called the information an important national security tool, as it was used to track the contacts of patients as well as those who did not comply with quarantine. ¹⁷⁵

Registration for a media briefing for social media users by the government-led National Development Media Centre required details like NIC numbers, even for users attending the briefings online. **176**

Following the Easter Sunday attacks, the government indicated its intention to ramp up monitoring and surveillance. During the coverage period, while speaking about the arrest of individuals for posts which allegedly referenced or promoted the LTTE propaganda (see C3), a government official said that the CID and TID deploy teams that monitor the internet and social media platforms. **177** In May 2019, the then prime minister announced a plan to implement a Centralized and Integrated Population Information System (CIPIS) to track individuals engaged in terrorism, money laundering, and financial crimes. **178** In August 2019, police announced that they were creating an integrated database and facial recognition system to “identify criminals” with SLT and other parties. **179**

In March 2021, it was announced that the Environmental Ministry had established a special unit of 323 officers to monitor posts on social media related to environmental destruction. **180**

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. **181** There has been no update on the practical 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. **182** Activists warn that this data could be used to target political opponents and is vulnerable to hacking. **183** President Rajapaksa has asked that the project be expedited. **184** 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. However, communications can be intercepted on the order of a minister or a court, or in connection with a criminal investigation.

State agencies reportedly possess some technologies that could facilitate surveillance. In March 2019, then president Sirisena requested approval for the government to

purchase 7.11 trillion rupees (\$38.9 million) 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. ¹⁸⁵

In 2015, leaked documents indicated that Milan-based HackingTeam was approached by several state security agencies seeking to acquire the company’s digital surveillance technologies. ¹⁸⁶ The leaks revealed that in 2014, the Defense Ministry was planning to develop an electronic surveillance and tracking system with the help of a local university. ¹⁸⁷ While no equipment purchases 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 previously brokered. ¹⁸⁸ Digital activists in Sri Lanka believe that Chinese companies ZTE and Huawei, which collaborated with Mahinda Rajapaksa’s government in the development and maintenance of the Sri Lankan ICT infrastructure, may have inserted backdoor espionage and surveillance capabilities into the technology. ¹⁸⁹

C6 o-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users’ right to privacy?

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 in September 2019, although a final draft is not yet public. ¹⁹⁰ Some feedback on the initial draft noted that it was modeled on the European Union General Data Protection Regulation (GDPR). ¹⁹¹ A series of discussions on the bill led by the ICTA was held in June 2021. ¹⁹²

Amid COVID-19, the country has integrated its defense apparatus into its pandemic response. Military intelligence agencies have obtained personal data from mobile service providers to identify people who have interacted with patients or evaded quarantines (see C5). ¹⁹³ In May 2021, a Google form circulated on WhatsApp purported to collect data on those living in Dehiwala and Ratmalana who had not

received a vaccine. However, the Dehiwala Municipal Council later confirmed that the form was not initiated by them and threatened to take legal action against those who continued to circulate it. ¹⁹⁴

In 2013, Dialog chief executive 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.” ¹⁹⁵ In 2016, however, SLT engineers apparently defied orders from their superiors to install equipment purchased for surveillance. ¹⁹⁶ The nature and number of government requests for data is unknown, since there is no legal provision that requires officials to notify targets. Some companies disclose information; from July to December 2020, Facebook received 55 such requests; 44 of them legal-process related and 11 of them emergency disclosure requests. Facebook did not provide data in response to any of the requests. ¹⁹⁷ Twitter reported one request from the government for user data during the January–June 2020 period. ¹⁹⁸

In January 2018, SLT opened a Tier 3 National Data Center, ¹⁹⁹ which hosts local data and serves as a cloud computing service, although the country does not mandate data localization. ²⁰⁰

C7 0-5 pts

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

3/5

More cases of intimidation against both journalists and ordinary users were reported during the coverage period.

In March 2021, opposition parliament members claimed that web journalist Sujeewa Gamage, a contributor to the Siyarata news site, was abducted and tortured for information on sources and political contacts. A police spokesman later said the journalist had made false claims of being abducted, adding that the Colombo Crimes Division would be questioning him and the two opposition members. ²⁰¹

Journalists are frequently the targets of assault, intimidation, and harassment. In April 2021, freelance photographer and activist Malika Abeykoon was arrested after covering a protest of health-care workers. He said he was beaten by a police officer

while in detention. **202** In October 2020, two Tamil Guardian correspondents, Kanapathipallai Kumanan and Shanmugam Thavaseelan, were assaulted while investigating an alleged timber trafficking operation in Mullaitivu. The journalists' attackers deleted most of the documentation of the deforestation and removed the journalists' memory cards. The attackers also stole their money and jewelry and filmed the journalists on their mobile phones while accusing them of trespassing. **203** In August 2020, Vijayanathan Janarthan, a media correspondent at Tamil newspaper and website *Valampuri*, was intercepted by two masked men on a motorcycle and attacked using barbed wire. **204** Journalists with online news sites theleader.lk and VoiceTube were also summoned and questioned at length by the CID (see C3).

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 LTTE members living abroad. **205** In December 2019, 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. **206** 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. **207** In November 2019, police raided the office of news site 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. **208** In May 2019, Kanapathipillai Kumanan, a freelance correspondent with the Tamil Guardian news site and the *Virakesari* newspaper, was assaulted by a police officer. **209**

Intimidation and harassment also increased around the COVID-19 pandemic. In June 2021, the CID was reportedly forming a team to act against the spread of misinformation on COVID-19 and other "sensitive" issues and take action against those who create and share purportedly false information. **210** The Free Media Movement expressed concerns that the government was detaining users who posted pandemic-related social media comments, and noted that the government targeted users living in the north and east of the country. **211** Police visited the home of a student activist after he criticized the government on Facebook (see C3). **212** Separately, when social media users called to boycott Muslim businesses and spread allegations that Muslims were spreading COVID-19, they were not refuted by the

government. Senior government officials also implied that the virus was rife among the Muslim community, drawing condemnation from civil society. **213**

Families of journalists have been targets of 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. **214**

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. **215** In the past year, there have been 400 cases of blackmail for money or sexual favors, sale of intimate videos to pornography websites, the leaking of intimate videos by former partners, sharing of obscene photos and videos, and the posting of edited photographs on social media. **216**

Female activists, lawyers and politicians have also endured threats and intimidation online that have affected their work. **217** A female lawyer who appeared on behalf of the families in an enforced disappearances case was threatened with violence and sexualized abuse on social media. **218** During the August 2020 elections, women candidates were also subject to sexualized abuse online. **219** Two Tamil women who were planning to contest the elections were aggressively attacked online. **220** Members of the LGBT+ community were also the target of hate speech and were "outed" online.

C8 0-3 pts

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

1/3

Score Change: The score declined from 2 to 1 due to the cyberattacks directed at online news outlets and multiple cases of government websites, including the prime minister's website, being hacked.

Government and business websites are vulnerable to hacking and other cyberattacks. While the problem is not historically widespread in Sri Lanka, notable attacks on government websites and other websites were recorded during the coverage period.

Cyberattacks occasionally targeted government critics, such as the TamilNet news site, under former president Mahinda Rajapaksa. **221**

In April 2021, the Colombo Gazette's news site was subject to a DDoS attack. The motivations of the attack were unclear. The editor speculated that the site was targeted by China because the botnet which launched the attack appeared to have originated from China and Hong Kong. However, because the attackers used CloudFlare technology, a subsequent IP trace was redirected to the closest CloudFlare server, which was in China; other experts, therefore, did not support the claim that China launched the attack. **222**

In February 2021, shortly after Independence Day, some users accessing Google.lk were redirected to another site which highlighted minority rights issues. The TRCSL called the incident a "malicious redirection" and said it was working with the Sri Lankan domain registry to resolve the issue. **223** It was later revealed that the domain registry's usernames and passwords had been leaked on the dark web, and that the credentials had been used on multiple sites since 2012, opening up the potential for future attacks. **224** The registry reported that several government agency websites were being redirected. **225** In a notice on its site, the registry acknowledged security shortcomings and noted they had since updated their systems to remove vulnerabilities. **226**

In May 2021, recognized as the anniversary of the end of the civil war, several websites were hacked by the Tamil Eelam Cyber Force. The Health Ministry, Energy Ministry, the Sri Lankan embassy in China, and the Rajarata University websites were affected. **227** The prime minister's website was hacked in June 2021, with the website redirecting to a site dedicated to the cryptocurrency Bitcoin. **228**

In June 2020, 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. **229** This allows the hacker to access the targeted person's two-factor authentication. Those affected included members of the Groundviews WhatsApp group, which was subsequently shut down, and potentially other journalist WhatsApp groups. In May 2021, the TRCSL issued a notice that SIM-swapping attacks continued to occur on WhatsApp. **230**

The draft Cyber Security Act, which would establish a Cyber Security Agency and implement the National Cyber Security Strategy of Sri Lanka, is expected to include provisions for protection against hacking (see C2). ²³¹

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. ²³² In May 2019, several local websites, such as that of the Kuwaiti embassy in Colombo, were defaced by unknown hackers. ²³³

Footnotes

- 1 Telecommunications Regulatory Commission, “Statistics,” March 2021 <https://trc.gov.lk/images/pdf/StatisticalOverViewReportQ1202105052021ab...> ,
- 2 “Vistas of Prosperity and Splendour,” Gotabaya Rajapaksa December 2019, <https://gota.lk/sri-lanka-podujana-peramuna-manifesto-english.pdf>
- 3 “Current Projects,” Information and Communication Technology Agency, <https://www.icta.lk/current-projects/>
- 4 “Wi-Fi Hotspots in Sri Lanka”, Dialog, <https://www.dialog.lk/wi-fi-hotspots>
- 5 Dialog invites customers to experience the power of 5G on trial network Daily FT July 22, 2020 <http://www.ft.lk/it-telecom-tech/Dialog-invites-customers-to-experience...>

More footnotes



On Sri Lanka

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

See More >

Country Facts

Global Freedom Score

56/100 **Partly Free**

Internet Freedom Score

51/100 **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 2021

Other Years

2020

Be the first to know what's happening.

Join the Freedom House monthly newsletter

Email

Subscribe

ADDRESS

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

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org

@2022 FreedomHouse