Freedom House

FREEDOM ON THE NET 2019

Myanmar

NOT FREE

36 /100

A. Obstacles to Access	10 /25
B. Limits on Content	16 /35
C. Violations of User Rights	10 /40

LAST YEAR'S SCORE & STATUS

36 /100 **Not Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Overview

Internet freedom remained constrained in Myanmar during the coverage period, as the government sustained its assault on free expression online. The military and ruling party continued manipulating online content, while users were hesitant to discuss sensitive topics such as gender, the mostly Muslim Rohingya ethnic group, or conflicts in Rakhine, Shan, and Kachin states. Worryingly, some individuals who criticized the government online faced prosecutions and even prison time under a range of laws, including the repressive Telecommunications Law.

Myanmar's transition from military dictatorship to democracy has faltered under the leadership of the National League for Democracy (NLD), which came to power in relatively free elections in 2015 but has failed to uphold human rights or bring security to areas affected by armed conflict. The military retains significant influence over politics, and the country is under international pressure regarding a 2017 military operation that forced more than 700,000 members of the Rohingya minority to flee to Bangladesh.

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

- The government continued to arrest and prosecute internet users for political speech, including Aung Ko Ko Lwin, who was sentenced to one year in prison in September 2018 for Facebook posts criticizing a state chief minister (see C3).
- In September 2018, Reuters journalists Wa Lone and Kyaw Soe Oo were sentenced to seven years in prison for their reporting on atrocities against the Rohingya, following a politically motivated trial; they were later pardoned in May 2019 (see C3).
- A range of draft laws could impact internet freedom and free expression, including a draft cybersecurity law proposed in 2019 (see C2 and C4).
- New reporting in October 2018 described a five-year-long systematic

disinformation campaign by nearly 700 military officials (see B5).

A. Obstacles to Access

Internet access continues to improve in Myanmar, as more users connect via smartphones with fast 4G service. The success of two foreign-owned mobile service providers has placed pressure on the state's monopoly, and the government has responded by giving a mobile phone license to a military-owned conglomerate and restoring the state's majority control over the mobile market.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**2**/6

Access to the internet continued to improve during the reporting period. Two-fifths of the population now uses the internet as of 2019, an increase of 17 percent or three million people since 2018. **1** The speed and quality of service increased due to the launch of 4G services in 2017, **2** and international bandwidth reached 445 Gbps in 2018, 15 times higher than 2013. **3** However, the overall number of users remains lower than the average for the Asia-Pacific region, **4** and both average internet speed and bandwidth per user are also lower than the regional average. **5**

Private fixed-line internet connections remain rare, and while fixed-line speeds increased during the coverage period, they are now on average less than half the speed of mobile connections. **6** Only 1 in 1,667 people has a fixed broadband line, compared to 1 in 10 on average across the Asia-Pacific region. **7**

The number of mobile connections has continued to grow, **8** increasing by about 7 percent in 2018, reaching 56 million connections in total. **9** Despite this growth, the percentage of the population with a mobile connection is lower than in neighboring countries. **10** Just over 50 percent of the population has mobile connections, and many people have multiple SIM cards. **11**

Infrastructure development continues to be a challenge, with flooding and unreliable electricity hampering connectivity, while an inefficient bureaucracy and corruption limit growth and improvement in the sector. [12] New sanctions adopted in the wake of the Rohingya crisis have also been applied to the export of telecommunications equipment to Myanmar, although it is unclear whether or how the sanctions have affected infrastructure development. [13] Meanwhile, infrastructure has been damaged by a range of problems such as rodents, car accidents, and construction. [14]

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

The internet became accessible to more people during the coverage period. The price of mobile internet connections has dropped and data is now more affordable. [15]

Prices for fixed broadband lines have continued to decrease, dropping on average by half between 2018 and 2019, though prices vary by region. [16] The costs of fixed-line connections have decreased due to competition with 4G and a dearth of demand from customers. The average fixed-line connection now costs $38 per month in urban areas, which remains prohibitively expensive for the majority of the population.

The Digital Economy Development Committee (DEDC) was launched in 2017 to support and develop economic policies that promote a digital economy. [17] In March 2019, the DEDC launched its Digital Economy Roadmap, which includes several plans to build digital inclusivity, improve connectivity, and harness technology to foster socioeconomic development. [18] The DEDC had met only twice by the end of the coverage period and has thus far largely operated in secret, without significant public consultation. [19] Although the roadmap divides responsibilities among different ministries, it is unclear how much—if any—budget has been allocated to operationalizing it.

National figures on internet access hide a digital divide that affects marginalized groups. Urban users who have access to 4G consume almost five times more data on average each month than the national average for all users. [20] The number of households, particularly in rural areas, that have access to a computer or to the internet remains small. [21] Users in rural areas and small towns have poorer internet connections than those in urban areas.

In recognition of the geographical disparity in access, the government announced the development of a Universal Service Fund (USF) to invest in telecommunications services for areas that are otherwise underserved, with the eventual aim of reaching 99 percent of the population. [22] The USF is supported by a new 2 percent telecommunications tax that was rolled out in mid-2018. [23] Four townships in the Rakhine and Magwe regions have been selected for the USF's first pilot project, [24] and the government is conducting a tender to identify service providers for the pilot. [25]

Gender-based disparities in access are generally ignored by the government. Women are still less likely than men to own a mobile phone and significantly less likely to use the internet. [26] The percentage of those aged 15 to 24 who use the internet is lower than in India, Indonesia, Thailand, Malaysia, Vietnam, and the Philippines. [27] For women, barriers to owning and using a mobile phone to access the internet include affordability, literacy skills, and security and safety concerns. [28]

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 has in the past refrained from restricting connectivity, [29] and there were no public reports of restrictions on connectivity during the coverage period. [30] However, in June 2019, after the coverage period, the government cut off the internet for over a million people in parts of Rakhine State and Chin State, areas where the military has conducted crackdowns, first against the Rohingya, and more recently against the Rakhine. [31] As of October 2019, the restrictions were still in

effect in some areas, affecting access for over 600,000 people.

The Ministry of Transport and Communications (MoTC) retains the power to cut off the internet without oversight or safeguards, as it owns and controls much of the telecommunications infrastructure via the state-owned Myanmar Posts and Telecommunications (MPT), although private providers are gradually diversifying ownership of mobile infrastructure and the internet backbone. Myanmar has seven internet gateways and is expected to develop more in the near future to support its 70 percent annual growth in bandwidth demand, **32** including new satellite connections planned for 2019. **33** New private internet gateways are making the international connection more resilient.

Myanmar has 68,000 kilometers of fiber-optic cable. **34** The first private undersea internet cable, the Myanmar-Malaysia-Thailand-International Connection (MYTHIC), was installed by Campana Group, a company based in Singapore and jointly owned by Myanmar and Thailand. It began selling wholesale to telecommunications companies in 2017. **35** Campana Group plans to build a second undersea cable, called SIGMAR, to be launched in 2020 with enough bandwidth to serve for at least 10 years. **36** Myanmar's government plans to launch a second satellite, MyanmarSat-2, in 2020 to support the telecommunications infrastructure. **37**

The legal framework has no specific regulations relating to bandwidth throttling, but many legal provisions are vague and broad, meaning that they can be misused for such purposes. **38** A draft cybersecurity law under consideration at the end of the reporting period could include restrictive provisions that affect Myanmar's internet infrastructure (see C2). **39**

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**2**/6

Although the government has awarded a number of telecommunications licenses, a military-owned telecommunications company has restricted the diversity of the market. Providers face a range of obstacles to effectively operate.

Myanmar has seen a proliferation of telecommunications licences awarded since 2013, when deregulation removed many of the legal and regulatory barriers to entry for internet service providers (ISPs) and mobile service providers. At least 137 telecommunications licenses had been awarded by the end of the coverage period, **40** and the share of subscribers using state-controlled mobile service providers briefly dropped below 50 percent during the coverage period. **41** However, the 2017 award of a telecommunication licence to the military-owned operator Mytel, and the comparative scale of Mytel's investment since launching in 2018, has undermined the diversity of providers and reasserted the state's dominance over the telecommunications market.

Mytel is jointly owned by the Vietnamese-military-controlled company Viettel, a consortium of local firms, and Star High Public Company, which is owned by the Myanmar military's Myanmar Economic Corporation (MEC). **42** The MEC was sanctioned by the US Treasury Department between 2008 and 2016 for its role in the human rights violations committed by Myanmar's military. **43** Mytel operates using the telecommunications infrastructure owned by MECTel, which is also owned by the MEC. **44** Some activists have called for a boycott of Mytel due to the company's connections with the military and human rights violations. **45** In 2018, the European Union considered applying sanctions to Mytel in response to the military's human rights abuses in Rakhine, Shan, and Kachin states. **46**

Mytel launched its 4G-only service in February 2018, **47** and had reached five million subscribers by 2019. **48** It joined three other mobile service providers in Myanmar, all of which are owned by the Myanmar government or foreign governments. **49** Two foreign mobile service providers, Telenor and Ooredoo, have market shares of 32.3 percent and 17.1 percent respectively as of the third quarter of 2018. **50** The state-owned MPT continued to shrink to a 47 percent market share by the third quarter of 2018. Other providers that have received telecommunications licences include a mixture of national and local fixed-line and mobile services. For example, Amara Communications, owned by a large domestic conglomerate, launched in May 2018 and provides a data-only service using MiFi boxes, including in Yangon, where it had already installed 300 towers by March 2018. **51** The Global Technology Group launched wireless broadband in 30 cities beginning in May 2018. **52**

The administering of licences is generally regarded as fair and transparent, and external efforts to influence decisions have been largely rebuffed. **53** Once given a licence, however, obstacles to operating effectively remain. Telecommunications providers have raised concerns about restrictions on building new towers, **54** and local government officials have stressed the need for providers to obtain permits to lay fiber-optic cables, build towers, and install Wi-Fi devices. **55**

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**1** / 4

Myanmar's regulatory bodies remain vulnerable to political interference and lack transparency. The MoTC's Posts and Telecommunications Department (PTD) is responsible for regulating the telecommunications sector. Under previous governments, the PTD was the regulator and a monopoly service provider for the telecommunications sector. These roles have now been separated, with the PTD acting as the regulator and the MPT acting as the state-controlled service provider. The PTD's responsibilities include issuing and renewing telecommunications licenses, regulating the frequency spectrum, addressing consumer protection, inspecting and supervising telecommunications providers, and carrying out any administrative actions against providers. **56**

However, both the PTD and MPT lack proper safeguards to protect regulatory and operational independence, making them vulnerable to political interference. Furthermore, the bodies' decision-making processes are opaque and they rarely engage or consult with civil society. **57** Article 86 of the 2013 Telecommunications Law outlines a Myanmar Communications Regulatory Commission (MCRC), which has yet to be established. **58** The MCRC, which would have insufficient safeguards for independence, would take over regulatory functions and institute a mechanism to adjudicate any administrative issues in the telecommunications sector. Many analysts believe that the government's failure to establish the MCRC is due to its unwillingness to relinquish direct control over the telecommunications sector. **59**

The Pricing and Tariff Regulatory Framework showcases how telecommunications rules favor state-owned service providers. The framework, an initial set of rules for mobile service providers, came into force in 2017 and included new floor pricing and a ban on offering free SIM cards or supplying telecommunications services below cost, among other rules. The rule on floor pricing included a minimum charge for data ($0.00065 per 1 MB of data), calls, SMS, and other services. The floor pricing, which was more expensive than some providers' prices at the time of adoption, was established for all providers to follow. However, the government waived floor pricing for the military-owned Mytel, reportedly to enable it to achieve rapid growth when it was first launched. **60**

Another state institution, the Myanmar Computer Federation, which was formed under the 1996 Computer Science Development Law and is comprised of industry professionals, is the designated focal point for coordination with technology-related associations, working groups, and other stakeholders in the sector. Civil society groups have raised concerns that the federation is progovernment and operates opaquely. **61** For example, the federation's leadership has supported some of the government's more draconian digital surveillance policies. **62**

B. Limits on Content

While the government continues to refrain from applying direct limitations on content, self-censorship on a range of subjects including the military, corruption, and the Rohingya, remains high. Social media companies have responded to pressure by opaquely increasing content removals, which has removed legitimate content. Users are free to access the internet, but there is a lack of diversity in the ownership and content of online media outlets. Meanwhile, the government and military actively promote their own narratives online and reject much independent reporting as "fake news."

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	**6** / 6

The government has continued to refrain from blocking or filtering content. In 2012, the government lifted all prior censorship of traditional and electronic media, with the exception of films, dissolving the Press Scrutiny and Registration Division shortly thereafter. The government does not actively publish blocking and filtering lists and there are no public reports about blocking or filtering during the period under review. Network measurements have not detected software used for censorship or manipulation of traffic inside Myanmar since 2012. **63** Political content appears to be almost universally available, and even content such as pornography was generally not blocked as of mid-2019. **64** Telenor, Myanmar's second largest mobile service provider in terms of subscribers and the only provider to publish annual transparency reports, reported receiving no requests to block content from the government during the coverage period. **65**

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?	**1** / 4

Pressure to remove content continues to originate from state and nonstate actors both within Myanmar and from outside the country. Google, Twitter, and Facebook have not reported any official requests for content removals from the government, including the courts. **66** Similarly, there are also no publicly available reports on formal government or court requests for publishers and content hosts to remove content.

However, the government employs other channels to pressure social media platforms and users. Government calls for content hosts and platforms, notably Facebook but also WhatsApp, to address rampant intolerance, misinformation, and incitement on their platforms continue. **67** But the government itself has failed to tackle these problems and often is responsible for perpetrating them. **68** Amid investigative reports on inflammatory online content that encouraged violence against the Rohingya people, there have also been international efforts targeting platforms to remove content, including from US lawmakers. **69**

As a result, Facebook has apparently increased its moderation practices and the use of its automated filtering mechanisms to remove content. **70** According to Facebook, it has removed hundreds of pages and accounts on Facebook and Instagram originating in Myanmar, with millions of followers, for violating its community standards. **71** Removals included the accounts and pages of Commander-in-Chief Min Aung Hlaing of the Myanmar Armed Forces, the military's Myawaddy television network, and other military leaders, **72** as well as nonstate actors such as the ultranationalist anti-Muslim monk Wirathu and pages run by the Buddhist ultranationalist group Ma Ba Tha. **73** The pages and accounts of the Arakan Rohingya Salvation Army (ARSA), Arakan Army, Myanmar National Democratic Alliance Army, Kachin Independence Army, and Ta'ang National Liberation Army were also removed because Facebook considered them "dangerous organizations." **74** This designation meant that any content and pages supporting these individuals or groups could also be removed once identified.

Activists, particularly women and religious minorities, reported being subjected to violence or threats intended to force them to remove their own content. **75** Pressure to remove content is also prevalent in coordinated reporting campaigns in which users misuse Facebook's mechanism for reporting content that violates the platform's community standards **76** in order to disable pages or temporarily limit users' ability to post or send messages. **77** Activists have argued that progovernment and military users have carried out a targeted campaign to report the content of pro-Rohingya and human rights groups.

B3 0-4 pts

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

A number of restrictions on digital content lack proportionality and transparency. The Telecommunications Law includes a broad provision giving the MoTC the absolute power to temporarily block and filter content "for the benefit of the people." **78** The law does not explicitly hold intermediaries liable for content, although some provisions are vague and could feasibly be used for content removal.

79 There are also no avenues for appealing restrictions, 80 and the only potential safeguard against abuse, the MCRC, has still not been established (see A5).

In lieu of the MCRC, the PTD retains control over content restrictions. It is not clear what content the PTD has restricted to date—if any—or whether there have been attempts to petition the PTD to reverse a decision. 81 ISPs and content hosts have not publicized any content restrictions, and the PTD does not publish procedural information on how or when any such decisions are made, and by whom.

Some concerned civil society organizations have suggested that Facebook's policies have become disproportionate, with the removal of entire accounts and pages rather than addressing specific issues, while providing no due process for those whose accounts have been removed. 82 Moreover, some activists argue that Facebook's actions have affected the public's right to information about important national stakeholders and swept up a wide range of legitimate content, including commentary on and documentation of human rights violations. 83 Despite regular requests from civil society, 84 Facebook is only minimally transparent about its restrictions.

In a welcome development, in April 2018, Facebook established an appeals process and published its internal community standards enforcement guidelines, 85 although it does not publish substantial information about content removal decisions. The public generally learns about removals through media reports. Some in civil society suspect that such opacity masks significant problems, such as poorly trained staff who lack contextual and language expertise, problematic and insufficient algorithms, 86 and disproportionate decision-making. 87

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Self-censorship online remains widespread, including among journalists 88 and women. 89 Journalists, online personalities, and ordinary users face a range of pressures to agree with government narratives on matters relating to the military, big business, armed conflict, religion, and certain sensitive social and religious issues. 90

The use of pseudonyms, which developed during military rule and enables people to speak out with less fear of repercussion, remains common online despite a ban on the practice by Facebook and other social media platforms. **91** Users are also learning to self-censor words and phrases deemed likely to be automatically identified and removed by content hosts such as Facebook, regardless of their legitimacy. **92**

Self-censorship is particularly common in discussing or reporting on the Rohingya. **93** For example, some journalists and media outlets have opted to use terms such as "Muslims" in order to lessen potential backlash online or, if the outlet is progovernment, the discriminatory term "Bengalis" is sometimes used, in an attempt to link the Rohingya to Bangladesh. **94** Pro-Rohingya activists have largely relied on social media and the international media to distribute information about violence and discrimination in Rakhine State, partly because few domestic media outlets are willing to take the security and financial risks of violence and boycotts associated with reporting on the crisis. **95** Despite their later pardon, the conviction of two Reuters journalists, Wa Lone and Kyaw Soe Oo, on politically motivated charges is a threat to other journalists and human rights defenders working on related issues (see C3), and has contributed to self-censorship. The fact that they work for Reuters, one of the world's largest media companies, has underlined the seriousness of the threat.

Self-censorship on gender issues is also widespread online among journalists and human rights defenders. **96** Women discussing sex and women's bodies online are often abused and harassed. **97** For example, while the global #MeToo campaign gained initial traction in Myanmar, some activists claim that survivors of sexual violence now often self-censor, having seen the intimidation faced by other women who have spoken out. **98**

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?	**1** / 4

The government and the military continue to dominate public discourse. Despite years of affirming their desire for media freedom, once in power, the ruling NLD resolved to retain state-run media [99] in order to control publicly available information. [100] As a result, the government and the military still control the entire broadcasting sector and a significant portion of print media, including those outlets' online publications, either directly through the Ministry of Information or via joint ventures with private companies. [101] Hopes that the NLD would increase the editorial independence of state-controlled media and joint-venture media outlets have evaporated. [102]

The government and military have sought to control information domestically. Manipulated progovernment content has become pervasive online, particularly on Facebook. [103] The military published inflammatory content regularly on Facebook before being banned by the platform in 2018 (see B2). [104] According to multiple sources, nearly 700 military officials were involved in a systematic campaign of misinformation for five years, creating and managing fake Facebook accounts and pages, which were then used to share false, misleading, and inciting content. Organized troll accounts allegedly helped spread the content to reach more users. [105]

The government continues to post on the Facebook pages of the Ministry of Information, [106] the State Counsellor Office, [107] and the Information Committee. [108] The latter was established to provide the public with "unbiased" information to combat "fake" reports from international media on the Rohingya and the conflict. It was originally called the "State Counsellor's Information Committee," before being renamed, reportedly either to demonstrate that the government is not dominated by Aung San Suu Kyi, [109] or to distance her from some of the page's more infamous pronouncements. [110]

Hard-liners have spread derogatory and violent statements about the Rohingya on Facebook, Viber, and WhatsApp, among other social media platforms. Before being banned by Facebook, the ultranationalist Wirathu used the platform regularly to spread false information and narratives. [111] His posts and videos, shared by thousands of followers, have, according to critics, stoked real-world violence. [112] He

has compared Muslims to mad dogs and shared images of corpses with text claiming they were Buddhists murdered by Muslims. **113** Other users have spread disinformation on social media that encourages violence. In 2017, thousands of Buddhist users were warned in Facebook messages of an imminent attack by Muslims, while Muslim users received similar messages saying Buddhists were about to attack. **114** Celebrities have also promoted virulent government messaging online. For example, a former Miss Myanmar, Shwe Eain Si, produced a graphic video in 2017 espousing the military's misleading account of the violence in Rakhine State, which blamed Rohingya militants for the crisis. **115** Civil society activists are concerned that disinformation will increase in the run-up to the 2020 general elections. **116**

Alongside propaganda, unintentional misinformation reflecting poor digital literacy or a lack of available and trustworthy information has spread.

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**1** /3

A number of laws contain provisions that can place regulatory constraints on users wishing to publish content online. While the provision has not been invoked to date, the 2014 Printing and Publishing Law created a licensing regime for publishing houses, news agencies, and websites, and outlets must register prior to producing content, including for publication online. **117** The law also contains a variety of vague and overly broad administrative and criminal sanctions for offenses, which include running a website without a license. Licenses can be revoked by the government at any time.

The Telecommunications Law has no specific regulations relating to net neutrality, zero-rating data transmissions by apps or telecommunications providers, or open internet policy. **118**

B7 0-4 pts

Does the online information landscape lack diversity?	1 / 4

Government and military control over public discourse and the media has significantly restricted the diversity of viewpoints online (see B5). Despite Facebook's removal of several official military accounts and pages (see B2), the military's messaging on certain issues, including conflict and minority groups, have continued to monopolize the online narrative. These viewpoints are presented on state-controlled broadcast media, and then feed into the public narrative on Facebook. Such content is then spread through users with military backgrounds or other promilitary accounts. **119**

The state's censorship efforts have also affected the diversity of online content produced by independent sources. For example, in 2019 the military requested that the media refrain from saying "civil war" when referring to domestic conflict. **120** In 2017, the government ordered that all media use the term "terrorist" instead of "insurgent" or "militant" when referring to the Rohingya crisis. **121** Also in 2017, the BBC announced that it would end its broadcasting partnership with MNTV after the network repeatedly pulled BBC programs for using "government restricted words," which included the word "Rohingya,"according to some analysts. **122** In June 2018, Radio Free Asia (RFA) cancelled its partnership with the Democratic Voice of Burma (DVB) after the government repeatedly attempted to censor the word "Rohingya" on state television. **123** RFA, however, reported that it would still cover Myanmar on social media. **124**

During the reporting period, the most-visited websites in Myanmar were Google, YouTube, and Facebook. **125** However, few people use internet browsers, with most users preferring Facebook apps on their mobile phones. The most popular Facebook pages were all run by media outlets, some of which were foreign and none of which were state-controlled. **126**

B8 0-6 pts

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

Online tools used to assemble and mobilize remain freely available. Individuals continued to use the internet for activism, some of which has been successful. Many within civil society regard Facebook as the best tool, and more effective than the mainstream media, to raise awareness about their concerns and prompt a government response. Their efforts have been constrained during the reporting period, however, as Facebook's restrictions on ethnic armed organizations, the military, and ultranationalist groups have impacted public discourse (see B2 and B3).

A number of online campaigns occurred during the coverage period. When the military leader Min Aung Hlaing, claimed in July 2018 that the military was more representative of the people than the elected government, a public outcry swept Facebook with the slogan, "The military doesn't represent me!" **127** After Reuters journalists Wa Lone and Kyaw Soe Oo were convicted in September 2018, Facebook profile pictures were replaced with black spots, representing blacked-out websites, and #ArrestMeToo trended on Twitter and Facebook. **128** In another example, the 2017 #SayNOto66d campaign **129** expanded in late 2018 to focus on decriminalizing defamation altogether. **130**

Some of the most significant online activism has been in response to the plight of the Rohingya. Pro-Rohingya digital activists have used social media to strengthen networks within the Rohingya community, including among the diaspora, while simultaneously reaching out to other supporters. **131** Social media has been invaluable for sharing videos, photos, and testimonies of sexual violence, looting, torture, and murder, **132** which mainstream media outlets have largely ignored.

C. Violations of User Rights

Criminalization of internet users persisted, including under several criminal defamation laws, while the government has hinted that a draft cybersecurity law could contain provisions punishing online criticism of the government. Intimidation

of users remains common, through online surveillance carried out by the government and military, as well as harassment against those reporting on or discussing conflicts in Rakhine, Shan, and Kachin states online, in addition to users discussing gender and other so-called "sensitive" issues.

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?	**1** / 6

The constitution and other laws in Myanmar fail to protect freedom of expression and press freedom. The current constitution, drafted by the military government and approved in a flawed 2008 referendum, states that "enhancing the eternal principles of justice, liberty, and equality" is one of the country's six objectives. **133** The constitution also provides specific—but highly limited—guarantees for citizens to "express and publish their convictions and opinions" **134** and "freely develop literature, culture, arts, customs, and traditions" **135** provided that they are "not contrary to the laws enacted for Union [of Myanmar] security, prevalence of law and order, community peace and tranquility, or public order and morality." **136** The constitution includes no provisions directly relating to the internet or access to information, although Article 96 and Schedule 1 (8.m) provide the parliament with authority to establish laws regulating the internet. In February 2019, the government established a joint parliamentary committee to review the constitution and put forward recommended amendments to bring it in line with democratic standards. **137**

Fair trial rights are often violated in Myanmar's courts, such as the accused not having effective representation and receiving limited access to court documents, and judges being inattentive during proceedings. **138** Trials relating to online activity commonly include significant procedural errors, technically unreliable evidence, and deep-seated judicial unwillingness to consult expert testimony. **139** In many cases, courts have been presented with easily-forgeable print-outs of digital content or have ruled without testing the authenticity, reliability, or admissibility of evidence. **140**

Judicial independence is impeded by interference. Judges are nominated by the president, and lawmakers can reject the choice only if it is clearly proven that the nominee does not meet the legal qualifications for the post. The courts generally adjudicate cases in accordance with the government's interests, particularly in major cases with political implications.

A number of laws target online media freedom. A 2018 amendment to the Broadcasting Law failed to clarify the country's transfer from analogue broadcasting to digital, which will result in an arbitrary process that could be misused by the government to control broadcasters and online media. **141** In 2018, the Myanmar Press Council, an independent body that settles disputes involving the media, submitted to the government a proposed amendment of the 2014 News Media Law, which regulates digital media. It remains unclear whether the proposal will positively or negatively affect media freedom. **142** A draft right to information law first proposed in 2017 had not yet passed by the end of the reporting period. **143** In June 2019, after the coverage period, a draft national records and archives bill that would limit access to information was introduced in the parliament. **144**

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	**0** / 4

Several laws explicitly penalize online activity and have been used to imprison internet users. The Telecommunications Law was drafted by the former government in 2013 with the support of the World Bank, **145** and is the primary framework for licensing telecommunications providers, including mobile service providers and ISPs. Although the law was welcomed by many stakeholders as a sign of much-needed change, **146** the former government added a number of troubling provisions, including Article 66(d), a vaguely worded content provision criminalizing a range of acts online, including defamation, and Article 68, which criminalizes "communication, reception, sending, distribution, or sharing of incorrect information with dishonest intention." **147**

Under public pressure about the number of prosecutions for online activity, the NLD government rushed through an amendment to Article 66(d) of the Telecommunications Law in 2017. However, the amendment was drafted without proper civil society consultation and was roundly condemned as insufficient. **148** Positive changes in the amendment include a reduction of the maximum prison sentence for violations from three years to two years, the opportunity for the accused to be released on bail, and restrictions on who can file a case. However, the amendment did not define defamation and did not alter provisions that outlaw "extort[ing], defam[ing], disturb[ing], or intimidat[ing]" over a telecommunications network. **149** Civil society activists have argued that the amendment has made no discernible impact on the cases brought after the amendment was enacted. **150**

The Law Protecting the Privacy and Security of Citizens, which was enacted in 2017 and widely condemned by civil society for being debated and passed without proper consultation, provides for prison terms of up to three years for defamation. **151** The law has been used to prosecute individuals for online activity (see C3).

The previous government amended but failed to repeal the 2004 Electronic Transaction Law (ETL) in 2013, which criminalized "any act detrimental to" state security, law and order, community peace and tranquility, national solidarity, the national economy, or the national culture—including "receiving or sending" related information. The law was routinely used to criminalize internet activism during military rule. In 2014, Thaung Tin, a senior government official, acknowledged the need to address repressive laws like the ETL and the Computer Science and Development Law, which criminalizes unauthorized use of a computer with a "fax-modem card." **152** The government announced plans to revise the ETL in 2014, but no draft legislation has since been announced. **153**

Several draft laws and amendments that could affect freedom of expression online were being considered at the end of the coverage period. In 2019, the government commissioned consultants to assist in developing a new cybersecurity law. **154** Initial drafts of the bill have been shared confidentially with a handful of civil society groups, but the legislation remained at an early stage of development at the end of the coverage period. **155** The government has stated that the new law will include

provisions penalizing those who "insult the country and people and commit crimes over any communications network." [156] Human rights defenders have expressed concern that the law, like other restrictive laws governing online activity in recent years, would be vague, overly broad, and used to punish a range of online behaviors. [157]

The Trademark Law adopted in January 2019 penalizes trademark infringement and counterfeiting with up to three years imprisonment and a fine of approximately 5 million kyats ($3,300). [158] It was adopted alongside the Patent Law and the Industrial Design Law, which also include criminal sanctions for violations. [159] In May 2019, a copyright law that includes prison terms of up to three years for commercial copying without consent was adopted. [160]

After a leaked draft law criminalizing "hate speech" received significant criticism from civil society, a new revised version was sent to the parliament in 2017, but the bill has not yet been passed. [161] The government claims that consultations with civil society regarding the bill have occurred, [162] but several well-known civil society organizations working on the issue have refuted these assertions and have received no responses to their requests for meetings with the parliament. [163]

C3 0-6 pts

Are individuals penalized for online activities?	**1** / 6

Internet users are frequently prosecuted in Myanmar's restrictive online environment. More than 200 criminal cases using Article 66(d) of the Telecommunications Law were filed between November 2015 and April 2019, [164] almost all of which were brought under the NLD government. [165] The majority of plaintiffs in the cases were affiliated with the state, including public officials, NLD party officials, and military officers, while the majority of the accused were activists, online journalists, or other civil society representatives. [166] Most cases have resulted in guilty verdicts with six-month prison sentences. [167]

One of the most notorious cases under Article 66(d) is that of Swe Win, the chief

correspondent for the news journal Myanmar Now, who was arrested in July 2017 for a Facebook post criticizing Wirathu, **168** after a complaint was filed against the journalist by a supporter of Ma Ba Tha, the Buddhist ultranationalist group. **169** Swe Win was forced to travel 600 kilometers from his home to the court more than 55 times, usually for a session that lasted just minutes. **170** The slow pace of Swe Win's proceedings has been common in Article 66(d) cases. The case was finally dismissed in July 2019, after the end of the coverage period, the chilling effect remains.

In May 2019, Reuters journalists Wa Lone and Kyaw Soe Oo were pardoned after serving more than 500 days in prison following their September 2018 convictions for reporting on the massacre of 10 Rohingya men and boys. **171** The journalists had been sentenced to seven years in prison for violating the Official Secrets Act. **172** They were originally detained in December 2017. In June and July 2018, the journalists' defense lawyers informed the court that they had been tortured while in custody (see C7).

In September 2018, Ngar Min Swe, a former columnist for state media, was convicted of sedition and sentenced to seven years in prison after he posted "abusive" Facebook posts about Aung San Suu Kyi. **173** His posts included sexist remarks about Suu Kyi after she received a kiss on the cheek from former US president Obama when he visited the country.

Also in September 2018, Facebook user Aung Ko Ko Lwin was sentenced to one year in prison for Facebook posts criticizing a state chief minister, under Article 8(f) of the Law Protecting the Privacy and Security of Citizens. **174** One post included a video clip in which the state minister controversially called on residents of the town of Thaton to "eat only a dish of curry" in hopes of lowering food prices. Aung Ko Ko Lwin was accused of "spoil[ing] the image of the town." **175** He was originally arrested in January 2018. **176**

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**3**/4

Users' ability to communicate anonymously is limited by the government's enforcement of SIM card registration requirements. **177** Since 2017, subscribers must provide their name, citizenship ID, birth date, address, nationality, and gender to register for a SIM card; **178** noncitizens must provide their passports. Shortly after the mandatory registration period began in 2017, the MoTC reportedly suspended six million unregistered SIM cards. **179** In March 2019, the government urged mobile service providers to limit each user to two SIM cards in order to protect "personal and national security." **180**

Although its provisions have not yet been implemented for web-only media outlets, the Printing and Publishing Law (2014) could potentially be used to prohibit anonymously run websites (see B6). **181**

There are no clear restrictions on encryption, although vague provisions in the Telecommunications Law and the Electronic Transactions Law could be interpreted to restrict the practice. Civil society activists are also concerned that the draft cybersecurity law could restrict encryption (see C2). **182**

C5 0-6 pts

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

Despite the fact that Article 357 of the constitution includes protection for private communications, government surveillance remains a serious concern. State surveillance of internet activities using sophisticated technology remains in its infancy in Myanmar because authorities continue to employ more invasive and direct methods to infringe on users' privacy. The police frequently confiscate the mobile phones of those facing allegations of online criminal activity without a warrant, particularly human rights defenders, political activists, and journalists. **183** The police reportedly demand passwords for social media accounts and other applications from suspects, including in cases where allegations are unrelated to social media use. **184** For example, shortly after Reuters journalists Wa Lone and Kyaw Soe Oo were arrested (see C3), the police were accused of using Wa Lone's confiscated phone to

send a WhatsApp message on his account. [185] The police used the Israeli phone-breaching product known as Cellebrite to collect data from the journalists' smartphones. [186] Cellebrite technology has been used by the police since 2016, and although the company ceased selling its products in Myanmar in late 2018, authorities continue to employ the technology. The revelations about Cellebrite also raised concerns about police accessing the journalists' social media accounts.

In February 2018, the parliament approved the creation of the Social Media Monitoring Team (SMMT), which was later established under the MoTC. [187] The government argued that the SMMT was necessary to counter those causing instability online, including through hate speech and defamation. [188] Public statements by senior government officials in May 2018 stated that the SMMT's mandate is narrowly focused on targeting foreigners and foreign organizations that cause unrest and threaten the country's sovereignty through interference. [189] Other analysts have suggested that, given Myanmar's broader political context, the SMMT was established to surveil foreign activists (including activists from Myanmar who operate outside the country or lack citizenship), foreign media outlets, and international organizations that focus on the Rohingya and the other conflicts Myanmar, as well as the International Criminal Court and other international bodies pushing for accountability for the atrocities against the Rohingya.

The SMMT was widely criticized by civil society organizations. [190] Despite the criticism, the SMMT was awarded an initial grant of approximately $4.8 million, [191] which it has reportedly used to purchase surveillance technology. [192] The scale and sophistication of the technology is unclear, [193] and the government has refused to reveal from which country the equipment was purchased, citing security concerns. [194] No information has been shared regarding the SMMT's powers and responsibilities, relationship with law enforcement and the courts, or any potential safeguards such as independent judicial oversight. Little is known about the body's operations or whether there is any oversight. [195]

The MoTC has announced its intention to build a data center in Naypyidaw, and in December 2018 the ministry requested that the parliament approve a $95 million loan from South Korea to fund the center, [196] which would serve as a secure base for

its planned e-government services. **197** The Mandalay regional government launched its data center in January 2019 to provide e-government services. **198** Concerns have been raised that the data centers will lack adequate privacy and security safeguards. **199**

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	**1** / 6

Service providers are increasingly concerned about protecting private data, given the ease with which the government can request it without proper oversight or appeals mechanisms. **200** International companies have also come under pressure; for example, a well-regarded NLD member of parliament has called for WhatsApp to monitor suspicious messages between users. **201**

The Law Protecting the Privacy and Security of Citizens, passed in 2017, prohibits the interception of personal communications without a warrant, but contains a vague exception allowing surveillance if permission is granted by the president or a government body. **202** The law does not outline clear procedures to prevent data from being collected and stored, nor does it provide for judicial review. Critics argue that the law's definition of privacy is inadequate and inconsistent with international human rights standards. **203** Laws demanded by a range of private sector and civil society stakeholders, including a robust data protection law, have not yet been proposed. **204**

The Telecommunications Law grants the government the power to direct unspecified persons "to secure any information or communication which may harm security, rule of law, or peace of the state." **205** The provision stating that any interception should not "hurt the fundamental rights of citizens" is an inadequate safeguard against abuse. **206** The Telecommunications Law also grants the government the power to inspect the premises of telecommunications license holders, as well as to require them to hand over documents, for the ambiguous purposes of defending the "security of the state or for the benefit of the people,"

without any safeguards against abuse. [207] A 2018 amendment to the Narcotic Drugs and Psychotropic Substances Law includes a new provision requiring telecommunications providers to disclose user information without due process. [208] There are no requirements for judicial review.

Telecommunications providers are generally reluctant to publicize the number of requests for data they receive from authorities. Telenor announced that in 2018, it received 64 requests for communications data and complied with 46. [209] In February 2019, new mobile service provider Mytel stated that it had thus far received 50 requests from the police for user data, "most" of which relate to human trafficking and drugs. [210] Some publicly available figures suggest that the number of requests for user data has decreased, but the percentage of requests fulfilled has increased. [211] One major provider stated that it initially required three documents before disclosing information, including a letter from a senior police officer and a letter from the PTD, but has in practice dropped the requirement for a court warrant. [212]

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?	**1** /5

Online journalists, human rights defenders, and political activists continue to report intimidation and threats of violence. In one opinion survey published in May 2018, most journalists reported that they believed violence against members of the media had increased compared to the previous year. [213] Violence and threats of violence were particularly common for journalists and activists reporting in conflict areas or communicating online about sensitive political issues such as the Rohingya crisis. [214]

Journalists reporting on the Rohingya crisis or working inside Rakhine State, where the majority of atrocities against the Rohingya have occurred, feel particularly targeted. [215] During the trial of Reuters journalists Wa Lone and Kyaw Soe Oo, defense lawyers informed the court that the journalists were tortured in detention. [216] In July 2018, Kyaw Soe Oo told the court that he was subjected to sleep deprivation and forced to kneel for hours while he was interrograted. [217] He also said

that authorities covered his head with a black hood. In 2017, Kyaw Lin, a journalist in Rakhine State who contributes to the DVB and is the editor-in-chief of the local outlet ROMA Time, was stabbed by two men on motorbikes. **218**

Human rights defenders also face intimidation and violence. The scale and volume of threats against human rights defenders, all of whom use the internet as their principal tool for advocacy, varies depending on the "sensitivity" of the issue. Pro-Rohingya and peace activists report high levels of intimidation via direct and indirect messages and comments online. **219** The government has itself perpetuated threats; in February 2019, a member of parliament threatened to take legal action against those who "damage the dignity" of the country by working with the United Nations. **220** In Myanmar, high-profile women and female human rights defenders report regular gender-based intimidation and threats of violence. **221** Common harassment tactics include cyberstalking, phishing, hacking, and attempts to cast doubt on women's credibility, integrity, and character. Many are intimidated through doctored sexual or intimate images, which are sometimes used in attempts to blackmail women.

A significant number of internet users have reported experiencing cyberbullying, particularly those in marginalized groups including young women, religious minorities, and the LGBT+ community. **222**

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

Websites, Facebook accounts, and email are periodically subjected to technical attacks in Myanmar. In 2017, websites for the Ministry of Culture, the Central Bank, and Maubin University, in addition to some private webpages, were hacked and populated with messages saying "Stop Killing Muslims." **223** The hacks were allegedly carried out by Turkish activists raising their concerns about the treatment of the Rohingya. **224**

Human rights defenders, journalists, and political activists continue to report regular, often weekly, remote attempts to hack their email and Facebook accounts. **225** Digital activists in Myanmar note that Google regularly warns them of "government-backed attackers" attempting to hack their Google products. **226** Pro-Rohingya and Muslim activists are among those who report frequent hacking attempts. **227** Police use sophisticated technology to hack into the devices of journalists, including Reuters reporters Wa Lone and Kyaw Soe Oo in 2017. **228** Advanced spyware has been identified in Myanmar, **229** and human rights defenders, journalists, and political activists report the use of spyware installed on their mobile phones. **230**

Microsoft has raised concerns once again about the large number of computers and devices in Myanmar that are infected by viruses and malware. **231** Almost 30 percent of computers in Myanmar are infected, compared to 18 percent globally. **232** Browser modifiers are twice as common in Myanmar than the global average, and software bundlers are almost three times more common. Microsoft has also raised concerns about the number of infections of the worm Win/Macoute that spreads to USB drives, which are very common in Myanmar, and communicate the drive's content to a remote host. **233**

Footnotes

5 The number of internet users was reported in 2019 a 18m by Internet World Stats, see "Internet Usage in Asia," Internet World Stats, https://www.internetworldstats.com/stats3.htm; A report on Myanmar in 2019 by Hootsuite identified that this number had grown to 21m users by the beginning of 2019, see "Digital 2019: Myanmar," Datareportal, accessed October 2, 2019, https://datareportal.com/reports/digital-2019-myanmar. 39 percent of the population and a growth of 3m persons over the course of the year.

2 "Ooredoo Myanmar and MPT step up 4G offerings," Developing Telecoms, June 6, 2017, https://www.developingtelecoms.com/tech/wireless-networks/7110-ooredoo-....

3 "Myanmar to accelerate 5G development despite risks," Eleven Media Group, December 19, 2018, https://elevenmyanmar.com/news/myanmar-to-accelerate-5g-development-des....

4 One index rates the percentage of the population using the internet as 33.1 percent in 2019 as compared to 51.8 percent for the Asia region, see "Internet Usage in Asia," Internet World Stats, accessed October 2, 2019, https://www.internetworldstats.com/stats3.htm; Others rate Myanmar as 39 percent, South-East Asia as 63 percent, and Asia as 52 percent,

see "The Global State of Digital in 2019 Report," Hootsuite, accessed October 2, 2019, https://hootsuite.com/pages/digital-in-2019.

Compared to other countries Myanmar has remained the same over the past year, see "Speedtest Global Index," Speedtest, accessed October 2, 2019, https://www.speedtest.net/global-index/republic-of-the-union-of-myanmar. In 2017, international internet bandwidth per Internet user was 6,426 (Bit/s) compared to 48,000 for Asia Pacific, and 6,000 for LDCs, see "ICT Development Index 2017," International Telecommunications Union, http://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-ta....

More footnotes

On Myanmar

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

See More ›

Country Facts

Global Freedom Score

9 /100 **Not Free**

Internet Freedom Score

12 /100 **Not Free**

Freedom in the World Status

Partly Free

Networks Restricted

Yes

Social Media Blocked

No

Websites Blocked

No

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2019

Other Years

2022

Be the first to know what's happening.

Join the Freedom House weekly 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