Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**369**
Land:	Myanmar
Kilde:	Freedom on the Net 2021 – Myanmar
Titel:	Report on digital media and internet freedom (reporting period June 2020 - May 2021)
Udgivet:	21. september 2021
Optaget på baggrundsmaterialet:	11. januar 2022

Freedom House

Myanmar

FREEDOM ON THE NET 2021

NOT FREE

17
/100

A. Obstacles to Access	4 /25
B. Limits on Content	7 /35
C. Violations of User Rights	6 /40

LAST YEAR'S SCORE & STATUS
31 /100 **Not Free**

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

Overview

TOP

Internet freedom in Myanmar collapsed following the February 2021 military coup, marking the most severe decline ever documented in

Freedom on the Net. As part of its attempt to crush dissent and maintain power, the military junta shut down internet service, blocked social media platforms and websites, seized control of the telecommunications infrastructure, and ramped up intrusive surveillance. Despite these and other obstacles, including detentions and egregious physical violence, people in Myanmar continued to use digital tools to organize and voice opposition to the coup whenever possible.

Myanmar's transition from military dictatorship to democracy had stalled under the leadership of the National League for Democracy (NLD) party, which came to power in relatively free elections in 2015. The military retained significant influence over politics under the constitution it drafted, and the government largely failed to uphold human rights and to prioritize peace and security in areas affected by armed conflict. A 2017 military operation and ongoing violence has forced hundreds of thousands of people from the Rohingya ethnic group to seek refuge in Bangladesh, and those remaining in Rakhine State continue to face the threat of atrocity crimes. Despite significant flaws and disenfranchisement, the November 2020 parliamentary elections resulted in a convincing victory for the NLD and a major defeat for the military-backed Union Solidarity and Development Party (USDP). That party's claims of fraud were cited as justification for the ensuing coup, in which the military ousted the NLD-led civilian government.

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

- The military began shutting down internet services nationwide shortly before the February 2021 coup (see A3), and in the subsequent months it seized direct control over state-owned mobile service providers that accounted for more than half of all mobile subscriptions in the country. Parallel pressure on private-sector providers was so severe that Norway's Telenor, one of the market leaders, sold off its mobile operations in Myanmar shortly after the coverage period (see A4).

TOP

- The ruling junta also assumed control over Myanmar's telecommunications regulator, quashing any independence it previously had through a series of opaque directives and threats to staff (see A5).
- Military authorities ordered the blocking of social media platforms, online news outlets, and certain financial-services websites, with some remaining inaccessible at the end of the coverage period (see A3, B1, and B3). As of June 2021, the military had revoked the licenses of seven major media outlets that were reporting on anticoup protests, and telecommunications companies were ordered to block their websites (see B1 and B6).
- The coup leaders' efforts to disrupt internet service and block online platforms were intended in part to suppress the organization of further protests. Authorities also banned virtual private networks (VPNs) and employed detentions and physical violence to punish users who expressed support for the anticoup movement. Nevertheless, citizens continued their attempts to mobilize via digital tools (see B8 and C4).
- The coup effectively nullified the constitution and the limited free expression protections it had offered, and the country's Constitutional Tribunal—tasked with holding state officials accountable under the charter—was replaced by the military days after it seized power (see C1).
- In March and May 2021, new evidence supported suspicions that the military was using extraction and interception technology to surveil protesters. The military also suspended limited privacy protections provided by the Law Protecting the Privacy and Security of Citizens and issued an amendment to the Electronic Transactions Law that increased government access to personal data (see C5).
- Journalists, digital activists, and ordinary users were held in pretrial detention and sentenced to prison terms for their online activity in the months following the coup. One Democratic Voice of Burma reporter received a three-year sentence in May 2021 in connection with his coverage of protests (see C3). Physical violence and torture have become widespread in detention, and disappearances of or public

TOP

attacks on prominent social media users served as additional deterrents to the expression of dissent online (see C7).

A. Obstacles to Access

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 coverage period, until the February 2021 coup. As of 2021, 43 percent of the population used the internet, an increase of two and a half million people since the beginning of 2020. [1] The speed and quality of service have increased in recent years due to the launch of fourth-generation (4G) mobile networks in 2017, [2] and international bandwidth reached 2,036 Gbps in 2020. [3] However, penetration overall remains lower than average for the Asia-Pacific region, [4] and internet speeds are slower than average, particularly for fixed-line connections. [5] The Ministry of Transport and Communications (MoTC) Universal Service Strategy for Myanmar 2018–22 aimed to reach 95 percent of the population with mobile broadband services and 99 percent of the population with basic mobile voice services by 2022. [6] At the end of the coverage period, achieving this goal appeared unlikely, especially in light of the coup.

Private fixed-line internet connections are rare, and while fixed-line speeds increased during the coverage period, they remain slower than mobile connections. [7] In 2020, just 0.5 percent of internet subscribers used fixed lines, a number that had not changed for five years. [8] Since the beginning of the COVID-19 pandemic in early 2020, the number of wireless broadband devices has grown in urban areas, as the need to work from home has increased. [9]

TOP

The number of mobile connections has also continued to grow, increasing to 69 million in January 2021, for a penetration rate of 127 percent. [10] Despite this growth, the share of the population with a mobile connection is lower than in neighboring countries. [11] Just over 50 percent of

residents have mobile connections, though many people have multiple SIM cards, accounting for the nominally high penetration rate. [12]

Infrastructure development continues to be hampered by flooding, unreliable electricity, an inefficient bureaucracy, and private- and public-sector corruption. [13] New international sanctions adopted in the wake of the military's 2017 campaign against the Rohingya population have affected the export of telecommunications equipment to Myanmar, although it is unclear whether or how the sanctions have obstructed infrastructure development in particular. [14] Existing infrastructure has also been damaged by a range of problems such as rodents, car accidents, and construction. [15]

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 prior to the coup. Mobile data plans are affordable relative to other countries in the region. [1] Deals offering free or near-free mobile access to social media platforms initially fed the rapid growth in Facebook usage and, after 2020, a similar explosion in TikTok usage. [2]

Prices for fixed broadband lines have continued to decrease, dropping on average by more than half between 2018 and 2021, though prices vary across different parts of the country. [3] The costs of fixed-line connections have decreased due to competition with 4G mobile service and a dearth of demand from customers. While the average fixed-line connection now costs $27 per month in urban areas, this remains prohibitively expensive for the majority of the population. [4]

TOP

The Digital Economy Development Committee (DEDC) was established in 2017 to support and develop economic policies that promote a digital economy. [5] 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. [6] Although the roadmap divides responsibilities among different ministries, it is unclear whether or how much funding has been allocated to implement the strategy. In 2020, there were reports that the DEDC was reemerging after a long period of opaque and infrequent activity, with a new focus on technical skills provision. [7]

National figures on internet access hide a digital divide that affects marginalized groups. Urban users who have access to 4G service consume almost five times more data on average each month than the national average for all users. [8] The number of households that have access to a computer or to the internet remains small, particularly in rural areas. [9] Users in rural areas and small towns have poorer internet connections than those in urban areas. Disparities have likely increased following the coup, as services are affected differently by military directives. [10]

In recognition of the geographical gaps in people's internet access, the government announced the development of a Universal Service Fund (USF) in April 2018 to invest in telecommunications services for areas that are otherwise underserved, with the eventual aim of reaching 99 percent of the population. [11] The USF is supported by a 2 percent telecommunications tax that was rolled out in mid-2018. [12] At least some of the USF funding has since been reallocated to pay for a proposed biometric database for mobile subscribers (see C4), and the amount of the remainder is unclear. [13] A tender for implementing the first phase of the USF was announced in November 2020, [14] while the second and third phases have been suspended following the coup. [15]

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. [16] For women, barriers to owning and using a mobile phone to access the internet include perceived lack of relevance, high costs, and insufficient literacy skills. [17]

TOP

A3 0-6 pts

	0 / 6

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

Score Change: The score declined from 1 to 0 due to the military's repeated shutdown of internet services nationwide, as well as months-long blocking of social media platforms including Facebook, Twitter, and WhatsApp.

Before the February 2021 coup, the government had generally refrained from restricting connectivity across the country, despite implementing one of the world's longest internet shutdowns in Rakhine and Chin States beginning in 2019. Since the coup, military authorities have repeatedly shut down internet services nationwide.

The military began disrupting the internet shortly before the coup, starting in the early morning hours of February 1, 2021. At 8 a.m., all mobile data and some fixed-line internet access were cut off nationwide. [1] The military's first internet shutdown after the coup ended later that day, but was followed by a near-total shutdown at 10 a.m. on February 6 that lasted 30 hours. [2] Military authorities then implemented nightly shutdowns affecting fixed-line (fiber-optic and cable) connectivity on February 15, lasting from 1 a.m. to 9 a.m., until reports that access had been restored began to surface on April 28. [3] Although the internet was on during the day in this period, users reported frequent short-term outages and slow speeds nationwide. On March 15, the military shut down all mobile data connections, which continued through the end of the coverage period, [4] leaving only wireless broadband services and fixed-line services working during the daytime. [5] On March 18, the military shut down public Wi-Fi connections. [6] On April 1, the military ordered providers to shut down wireless broadband internet services indefinitely. Daytime fixed-line service, which is used by between 0.5 and 5 percent of users, was consequently the only way to access the internet. [7] TOP

Months-long blocks on various social media platforms were ordered by the military in a bid to further control the flow of online information surrounding the coup (see B1). The military began listing some 1,200

approved internet services on May 25, which included a number of the previously blocked platforms. [8]

Before implementing the national shutdowns, the military briefly ended one of the world's longest internet disruptions at the subnational level. On February 2, 3G and 4G mobile access was restored to 1.4 million people in Rakhine and Chin States. [9] The government in June 2019 had cut off mobile internet service in these areas—where the military has conducted crackdowns over the past several years, first against the Rohingya and more recently against the Rakhine ethnic group—in order to "maintain the stability and law and order." [10] The government had pledged to restore access when the security situation improved, [11] and a presidential spokesperson had said that the government would "fulfill every request made by" Myanmar's military with regard to the shutdown in the two states. [12] The government had restored limited 2G access in August 2020.

The MoTC directed the internet shutdowns, apparently under orders from the military-controlled Ministry of Home Affairs (MoHA). [13] In the first few days after the coup, one telecommunications company documented the existence of the directives, which cited "fake news" and the need to protect national stability. [14] The company stopped documenting the directives it received, [15] however, reportedly due to license-related pressure from the MoTC (see B3). There were already reports that the MoTC had been pressuring telecommunications companies prior to the coup, [16] and these reports have increased since. [17]

The MoTC has significant powers to cut off the internet without oversight or safeguards, as it controls much of the telecommunications infrastructure via the state-owned company Myanmar Posts and Telecommunications (MPT). Private-sector providers were gradually diversifying ownership of mobile infrastructure and the internet backbone. Myanmar has three underwater and four overland internet gateways. [18] Because experts projected that bandwidth demand would grow 70 percent annually in the near future, before the coup more companies expected to develop infrastructure, [19] including through new satellite

TOP

connections. [20] Since the coup, there has been no progress toward these goals.

Myanmar has 68,000 kilometers of fiber-optic cable and 11,000 more under construction. [21] The first private undersea internet cable, the Myanmar-Malaysia-Thailand International Connection (MYTHIC), was installed by the Campana Group, a company based in Singapore and jointly owned by Myanmar and Thailand. It began selling wholesale access to telecommunications companies in 2017. [22] The Campana Group planned to build a second undersea cable, called SIGMAR, with enough bandwidth to serve for at least 10 years, [23] though little was known about the progress of the cable's development as of May 2021. Myanmar's government planned to launch a second satellite, MyanmarSat-2, in 2020 to support telecommunications infrastructure. [24] The satellite, built in a joint project with Hokkaido University in Japan, was held at the International Space Station following the coup, awaiting a Japanese decision as to whether it should be deployed at the risk of enabling military surveillance. [25]

The legal framework has no specific regulations related to bandwidth throttling, but many legal provisions are vague and broad, meaning they can be misused for such purposes. A draft cybersecurity law under consideration in recent years that was created by the government could include restrictive provisions that affect Myanmar's internet infrastructure (see C2). [26]

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**1** / 6

Score Change: The score declined from 2 to 1 due to increased military control over and pressure against providers, which led Telenor, one of the country's main providers, to write off its Myanmar operation as a total financial loss during the coverage period.

TOP

Since the coup, the military has seized control of the state-owned mobile operator, MPT, in addition to the military-owned operator Mytel. [1] As a result, the military is now in direct control of more than half of all mobile subscriptions as well as much of the telecommunications infrastructure, which is managed by MPT. [2] This has undermined the diversity of operators and, through the infrastructure, given the military a near monopoly in the telecommunications sector. Furthermore, the military, via the MoTC, has been issuing a significant number of directives to telecommunications companies, the legality of which the companies have questioned in many cases. [3] The volume and nature of the directives raised concerns among civil society actors about whether telecommunications companies are operationally independent from the military. Several stakeholders have confirmed that the military's detention of senior business leaders from other sectors likely encouraged telecommunications companies to implement military demands without complaint. [4]

The military pressure in the form of directives and threats to staff led one of the nation's main mobile providers, Norway's Telenor, to sell its Myanmar operations to a Lebanon-based company in July 2021, [5] after the coverage period. Telenor had written off its business in the country in May, essentially predicting a total financial loss, but said at the time that it would operate as long as it could still "contribute positively." [6]

Deregulation in 2013 removed many of the legal and regulatory barriers to entry for internet service providers (ISPs) and mobile service providers, leading to a proliferation in the number of licenses awarded. At least 207 telecommunications licenses had been awarded by 2020. [7] The 2017 award of a telecommunications license to the military-owned operator Mytel, and the comparative scale of Mytel's investment since launching in 2018, undermined the diversity of providers and reasserted the state's dominance over the telecommunications market. Independent media outlets have reported that Mytel provides the military with massive profits. [8]

TOP

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). [9] Mytel operates using the telecommunications infrastructure owned by MECTel, which is also owned by MEC. [10] MEC was sanctioned by the US Treasury Department between 2008 and 2016 for its role in human rights violations committed by Myanmar's military. [11] In 2018, the European Union considered imposing sanctions on Mytel in response to the military's human rights abuses in Rakhine, Shan, and Kachin States. [12] Since the coup, many activists have called for a boycott of Mytel due to the company's connections with the military and its human rights violations. [13]

Mytel launched its 4G-only service in February 2018, [14] and had reportedly reached 10 million subscribers by 2020. [15] It joined three other mobile service providers in Myanmar, all of which are owned by the Myanmar government or foreign governments. [16] During the coverage period, two foreign mobile service providers, Telenor and Ooredoo, had 22 and 10 million subscribers, [17] respectively, and a third provider, the state-owned MPT, had roughly 24 million subscribers. [18] Other providers that have received telecommunications licenses 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 wireless broadband boxes, including in Yangon, where it had already installed 300 towers by March 2018. [19] The Global Technology Group launched wireless broadband in 30 cities beginning in May 2018. [20]

Before the coup, the administration of licenses was generally regarded as fair and transparent, and external efforts to influence decisions were largely rebuffed. [21] However, in 2020 the government reportedly threatened to cancel licenses unless their holders complied with demands to block websites, including news outlets (see B1). [22] Telecommunications providers have raised concerns about restrictions on building new towers, [23] 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. [24]

TOP

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

Score Change: The score declined from 1 to 0 because regulatory bodies retain no independence following their takeover by military forces as part of the February 2021 coup.

Myanmar's regulatory bodies have reportedly been under the direct authority of the military since the coup. The MoTC's Posts and Telecommunications Department (PTD) is responsible for regulating the telecommunications sector. The PTD was once both the regulator and a monopoly service provider for the telecommunications sector. These roles were separated a number of years ago, with the PTD acting as the regulator and 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. [1] The whole of the MoTC, including both the PTD and MPT, is reportedly now influenced by the military-controlled MoHA. [2] Orders from the MoTC to providers to install interception spyware before the coup, for instance, came from former military officials (see C5). The nature of this management remains largely opaque, as the military does not publish the directives it issues (see A4, B1, and B3). [3] The military has also repeatedly and publicly threatened MoTC staff who have participated in strikes against the coup. [4]

Even before the coup, both the PTD and MPT lacked proper safeguards to protect regulatory and operational independence, leaving them vulnerable to political interference. For example, in March 2020, presidential spokesperson Zaw Htay said the government would "fulfill every request" made by the military regarding lengthy internet shutdowns in conflict zones (see A3). [5] Furthermore, the bodies' decision-making processes are opaque, and they rarely engage or consult with civil society. [6] Article 86 of the 2013 Telecommunications Law outlines the

TOP

responsibilities of a Myanmar Communications Regulatory Commission (MCRC), which has yet to be established. [7] Even though the mandate for the MCRC's composition does not sufficiently safeguard its independence, the Telecommunications Law calls for the MCRC to take over regulatory functions from the PTD. The commission would also operate a mechanism to adjudicate any administrative disputes in the telecommunications sector. Many analysts suggested that the government had long failed to establish the MCRC because it was unwilling to relinquish the more direct control it had over the telecommunications sector through the PTD. [8]

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 provisions. The rule on floor pricing included a minimum charge for data ($0.00065 per MB of data), calls, text messaging, 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. [9]

Another state institution, the Myanmar Computer Federation, was formed under the 1996 Computer Science Development Law and is composed of industry professionals. It is the designated focal point for coordination with technology-related associations, working groups, and other stakeholders in the sector. In the years prior to the coup, civil society groups raised concerns that the federation was progovernment and operated opaquely. [10] For example, the federation's leadership supported some of the government's more draconian digital surveillance policies. [11] Since the coup, the federation has spoken out to criticize the military's actions. [12]

TOP

B. Limits on Content

B1 0-6 pts

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?	**1** / 6

Score Change: The score declined from 3 to 1 due to open-ended blocking of social media platforms such as Facebook, WhatsApp, Twitter, and Instagram, as well as a range of websites, including news outlets, financial services, and gaming hubs.

The MoTC first began ordering telecommunications companies to block websites in March 2020, and blocking directives significantly increased following the coup. From February 2021 onward, the MoTC issued a series of orders requiring telecommunications companies to block access to URLs and internet protocol (IP) addresses under Section 77 of the Telecommunications Law, which allows authorities to issue blocking orders to license holders in "emergency situations." [1] Each of the directives are temporary but open-ended. No exact list of blocked sites has been published, and after Telenor publicly reported the directives it had received, it was forced to cease doing so under pressure from the authorities. [2]

The MoTC ordered all ISPs, mobile service providers, and international gateway managers to block access to Facebook on February 3, 2021. The block, which was initially set to last until February 7, was ostensibly meant to preserve stability and prevent fake news from "spreading misunderstanding." [3] WhatsApp was also blocked. [4] Orders to block Twitter and Instagram followed on February 5. [5] While WhatsApp and Instagram were included on a list of approved sites on May 25, Facebook and Twitter remained blocked at the end of the coverage period. [6]

Many more secretive blocks on websites have reportedly been ordered since the coup, affecting popular platforms such as Wikipedia as well as national media outlets (see B6). [7] At least one telecommunications company has reportedly pushed back against at least one MoTC order, with some success. [8]

TOP

On May 25, the military began listing approved sites, meaning any blocking on them could be removed. The initial batch of some 1,200 approved internet services included a large contingent of banking and financial sites, entertainment sites like YouTube and Netflix, news sites such as the *New York Times* and US-based Cable News Network (CNN), and gaming platforms. [9]

In March, May, and August 2020, the MoTC had issued a series of directives ordering internet providers to block more than 2,170 websites under Section 77 of the Telecommunications Law. Although the directives were not publicly released, well-known independent and local news outlets and websites based in conflict-affected areas, such as Rakhine State, soon became inaccessible. They included Narinjara News, Mandalay In-Depth News, Mekong News, and Voice of Myanmar, among others. Karen News, a local news agency in Karen State, was also found to be inaccessible. Several of the blocked outlets are owned by the Development Media Group, which previously had been targeted by authorities for its coverage of the rebel Arakan Army (see C3). [10] According to Telenor Myanmar, 67 websites were flagged for blocking in March 2020 for alleged "fake news," and 154 websites were accused of carrying adult or explicit content. The remaining 1,917 websites included in the MoTC's directives of March 2020 were also on Interpol's list of banned child sexual abuse websites; such content can be legitimately restricted under international human rights standards. [11] Justice for Myanmar, a campaign group that has criticized the military, was blocked in August 2020. [12] In May 2020, Telenor reported that the PTD had issued a directive ordering service providers to block an additional 22 websites that allegedly contributed to "fearmongering" and "misleading" people about COVID-19. [13]

Major telecom providers complied with the 2020 blocking orders. Telenor Myanmar initially resisted the blocking of 67 websites for alleged "fake news," citing the lack of a sufficient legal basis. [14] The provider later complied, however, after meeting with MoTC officials and determining that the "risk involved in not following the directive as regards fake news is likely to have wider implications in terms of servicing the public." [15]

TOP

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?	**1** / 4

Pressure to remove content continued to originate from state and nonstate actors within Myanmar, as well as from outside the country, throughout the coverage period. Since the February 2021 coup, pressure from the military against media outlets, including demands to cease critical coverage and halt the use of words translating to “regime” and “junta” (see B5), has led to the closure of two large media enterprises, with one opting to take down its entire website. [1] It is also believed that officials have pressured detained users to delete their own content while in custody. Separately, content moderation efforts by social media companies like Facebook, YouTube, and TikTok have led to the removal of content that should be protected under international human rights standards (see B3).

Prior to the coup, the government employed other channels to pressure social media platforms and users. Officials called for content hosts, notably Facebook but also WhatsApp, to address rampant intolerance, misinformation, and incitement on their platforms. [2] But the government itself had failed to tackle these problems, and individuals linked to the government were often alleged to be responsible for perpetrating them. [3]

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**0** / 4

TOP

Score Change: The score declined from 1 to 0 because directives to restrict content were issued en masse without transparency, proportionality, or an avenue for appeal.

Since the coup, broad restrictions on digital content have been enforced without transparency and with gross disproportionality. [1] Those who report on the existence of such restrictions have been threatened with severe consequences. [2]

Though the government vaguely described the aims of its restrictions before the coup, the military junta has generally not. The Telecommunications Law includes a broad provision giving the MoTC absolute authority to temporarily block and filter content "for the benefit of the people," although this power was never intended to be used to block all content. [3] The law does not explicitly hold intermediaries liable for content, but some provisions are vague and could feasibly be interpreted to justify content removal. [4] There are also no avenues for appealing restrictions, [5] and the only potential safeguard against abuse, the MCRC, has still not been established (see A5).

In the absence of the MCRC, the PTD retains control over content restrictions. The PTD does not publish procedural information on how or when any such decisions are made, or by whom. Military directives—and government directives before the coup—that order internet shutdowns and website blocks have not been published, and users have had to rely on telecommunications companies and civil society testing for more information about content restrictions. [6] The orders have become so common that many are conveyed to providers by telephone rather than through official channels. [7] Recipients of directives are unwilling to publicize the orders' exact terms due to the risk of legal liability, including potential violations of the Official Secrets Act, and there have been no reported legal challenges to test the directives' lawfulness in courts. The only ISP that had been documenting and publishing the existence of restrictive directives following the coup, Telenor, ceased those activities on February 14, citing threats of license revocation and intimidation of staff. [8]

TOP

In 2018, following complaints about its content moderation from within Myanmar and elsewhere, Facebook increased its moderation activity, expanded its appeals process for account and page takedowns, [9] and established a self-regulatory Oversight Board. [10] According to the

company, it subsequently removed hundreds of Facebook and Instagram pages and accounts—with millions of followers—that had originated within and outside of Myanmar and were found to have violated the platforms' community standards. [11] Removals in 2018 included the accounts and pages of top military commander Min Aung Hlaing, other military leaders, and the military's Myawaddy television network, [12] as well as accounts associated with the Buddhist ultranationalist group Ma Ba Tha. [13] After the coup, Facebook removed or reduced the distribution of many pages run by the military or military companies, including Tatmadaw True News Information Team, MRTV, and MRTV Live. [14] The pages and accounts of various ethnic rebel groups have also been removed by Facebook in recent years, as the company deemed them "dangerous organizations." [15] This designation meant that any content supporting the groups could also be removed once identified. An unintended consequence of Facebook's increased moderation activity has been the removal of legitimate content. [16]

Some activists continue to argue that some of Facebook's removals have compromised the public's right to information about important national stakeholders, and that they have swept up a wide range of valid content, including commentary on and documentation of human rights violations. [17] For example, certain media outlets, journalists, and human rights defenders have alleged that their content was wrongfully removed, particularly journalistic reporting about banned organizations. [18] Despite requests from civil society, [19] Facebook is only minimally transparent about its restrictions. Some in Myanmar's civil society sector suspect that this opacity masks significant internal problems, such as poorly trained staff who lack contextual and language expertise, problematic and insufficient algorithms, [20] and discriminatory decision-making. [21] The Oversight Board has agreed to review one case in which an appellant challenged Facebook's decision to remove a post criticizing the postcoup environment on the grounds that it violated the platform's hate speech policy. [22]

TOP

A 2020 survey of journalists conducted by Free Expression Myanmar found that Facebook had warned a third of the participants that their journalistic content violated the platform's community standards. [23] Of

those surveyed, 15 percent said they had content removed. Since the coup, several news outlets have reported receiving Facebook warnings after they posted photos of murdered protesters. [24]

In addition to Facebook, video platforms such as YouTube and TikTok have increased their content removals since the coup (see B5). [25] YouTube has removed at least five military-controlled channels, including the state-owned MRTV and the military-owned Myawaddy Media, MWD Variety, and MWD Myanmar. [26] Following international media attention, [27] TikTok slowly took action to remove some of the extremely violent videos posted by soldiers on the platform, many of which threatened peaceful protesters with various weapons and methods of murder. [28] In one video, viewed 180,000 times, a soldier says, “Don’t touch [the coup leader]. It will cost you your life. Hear? You will die.” [29] TikTok has been criticized by civil society for not learning the lessons from Facebook’s moderation failures in previous years. [30] While TikTok deleted many of the worst videos, technical glitches have left traces in place, and TikTok has not banned the military more broadly. [31]

B4 0-4 pts

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

Since the coup, self-censorship online has grown significantly. Although many social media users have bravely condemned the coup and continue to do so, some have apparently taken self-censorship steps to hide their identity, such as changing their account names or removing photos. [1] The practice of using acronyms or nicknames for sensitive terms is now widespread across messaging tools. [2] The use of pseudonyms, which was common during earlier periods of military rule and enables people to speak out with less fear of detention and criminal prosecution, has grown despite a ban on the practice by Facebook and other social media platforms. [3] Many users have also stopped using normal phone lines and switched to encrypted smartphone apps, such as Signal and Telegram. [4] Hundreds of journalists are in hiding, and many have been

TOP

detained for their journalism, particularly when reporting on the anticoup protests. [5]

Self-censorship was common prior to the coup, including among journalists. [6] Journalists, online personalities, and ordinary users faced a range of pressures to agree with government narratives on matters related to the military, major business groups, armed conflict, the Rohingya, religion, and other important topics. [7] For example, some journalists and media outlets opted to use terms such as “Muslims” when referring to Rohingya to avoid potential ultranationalist backlash online; the term “Bengalis” is also sometimes used in a discriminatory attempt to link the Rohingya to Bangladesh and deny their basic rights in Myanmar. [8] Pro-Rohingya activists largely relied on social media and the international news media to share information about violence and discrimination in Rakhine State, partly because few domestic media outlets were willing to risk the security threats or boycotts that can result from reporting on the topic. [9] Since the coup, more Myanmar users have actively spoken out about the Rohingya, in some cases apologizing for not believing past atrocity allegations in the light of the military’s recent violence against civilians protesting its seizure of power. [10]

Self-censorship on gender issues is also widespread online among journalists and human rights defenders. [11] Women who discuss sex and women’s bodies online are often abused and harassed. [12] For example, while the global #MeToo campaign against sexual assault and harassment 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. [13] Before the coup, some users, including those who discussed what are considered sensitive issues, had also learned to avoid words and phrases that might be automatically identified and removed by content hosts such as Facebook, regardless of their legitimacy; even innocuous words that contain slurs within their text could be affected. [14]

TOP

B5 0-4 pts

	1 / 4

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?

At the beginning of the coup, the military took control of all state-owned media and government communications channels. This entailed the capture of Twitter accounts and Facebook pages, including the Facebook page of the NLD. [1] The military has since used these outlets to disseminate its propaganda and threats. [2] Some of the Facebook pages and Twitter accounts, including those controlled by the Ministry of Information, have been suspended, either directly by the platforms or in response to user-generated reporting campaigns. [3] The military has also instructed the private media to report on the coup in a more supportive manner, and punished outlets that continued to criticize the junta. [4]

The military has repeatedly threatened to revoke media outlets' publishing licenses if they did not stop using Myanmar words that translate as "regime" and "junta." [5] A directive issued in February 2021 by the military-run Ministry of Information argued that the terms were inaccurate, as the junta's governing body was "constitutionally formed by the military." Editors and journalists with the *Myanmar Times* reported interference in their work as management banned terms like "coup," requiring the use of "power transfer" instead. [6] Most outlets continued their critical coverage, and the military had canceled the digital and print publishing licenses of seven large national outlets by June 2021, rendering them unlawful and leaving their staff at risk of arrest for unlawful association. [7]

The military and its affiliates spread manipulated information claiming electoral fraud following the November 2020 elections. Since the coup, the military has simultaneously warned against spreading rumors and faced numerous allegations that it promotes misinformation itself. [8] Even before it seized power, the military's messaging on certain issues, including on the Rohingya and other ethnic and religious minority groups, dominated the online landscape. These viewpoints had been presented on state-controlled broadcast media and fed into the public discourse on

TOP

Facebook. The content was then amplified by users with military backgrounds or other promilitary accounts. [9]

Despite years of affirming its desire for media freedom, the NLD sought to retain control over state-owned media during its time in government, [10] apparently to manage what information was publicly available. [11] As a result, the NLD-led government and the military dominated the broadcasting sector and a significant portion of print media prior to the coup, including those outlets' online presences, either directly through the Ministry of Information or via joint ventures with private companies. [12] They claimed to use official Facebook pages—such as those of the Ministry of Information, [13] the State Counsellor Office, [14] and the Information Committee [15]—to provide the public with "unbiased" information and combat "fake" reports from international media, often citing coverage related to the Rohingya people.

Major social media companies have attempted to limit the spread of manipulated information emanating from the military (see B3). YouTube removed some accounts run by the military and imposed limits on others for disseminating disinformation after the coup. [16] In February 2021, Facebook banned the remaining military accounts on its main platform and on Instagram, including those of military-controlled media outlets and companies. [17]

Military officials were also found to manipulate content during previous coverage periods. [18] The military regularly published inflammatory material on Facebook before being banned by the platform in 2018 (see B2). [19] According to multiple sources, nearly 700 military officials had been involved in a systematic campaign of disinformation 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. [20] In 2019, Facebook banned a number of pages and accounts for engaging in "coordinated inauthentic behavior," some of which were allegedly run by persons associated with the military. [21]

TOP

An article published after the coverage period in June 2021, however, found that Facebook's page-recommendation algorithm had been amplifying military content that violated many of its own violence and misinformation policies. [22]

Hard-liners who spread derogatory and violent statements about the Rohingya on Facebook, Viber, and WhatsApp, among other social media platforms, have widened their efforts to target other marginalized groups over the past several years. Before being banned by Facebook in 2018, the ultranationalist monk Wirathu, who is affiliated with Ma Ba Tha, regularly spread disinformation and false narratives through posts and videos that were shared by thousands of followers, and that allegedly stoked real-world violence. [23]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**0** / 3

Score Change: The score declined from 1 to 0 because the space for journalists and users to publish online has been dramatically diminished since the coup, especially as the military stripped major media outlets of their licenses in retaliation for their coverage.

Between the February 2021 coup and the end of the coverage period, the military revoked the licenses of seven major media outlets and ordered telecommunications companies to block their websites. [1] A state television outlet announced in March 2021 that five independent media companies—Myanmar Now, Khit Thit Media, Democratic Voice of Burma, Mizzima, and 7Day News, all of which had been covering the anticoup protests—were "no longer allowed to broadcast or write or give information by using any kind of media platform or using any media technology." [2]

TOP

The 2014 Printing and Publishing Law created the licensing regime for publishing houses, news agencies, and websites, and these outlets must register prior to producing content, including for publishing online. [3] The

law also contains a variety of vague and overly broad administrative and criminal sanctions for violations, such as running a website without a license.

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

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	**1** / 4

The diversity and reliability of information online are significantly restricted.

Since February 2021, the vast majority of new information disseminated online has focused on the coup. Much of this information has come from citizen journalists documenting the military's increasingly violent crackdown and the people's creative responses. [1] Public demand for information about the coup has simultaneously increased, and media outlets that provide it have garnered greater attention and respect. [2] Fact-checking and verification have become easier on the one hand, due to the number of sources, and more difficult on the other, because journalists cannot easily travel and have no access to official responses from the state. [3]

As independent media have become harder to access online, and only the propaganda of state-controlled media is available on television and radio, false and misleading information about the state's activities has become more common (see B5). Particularly prevalent rumors on Facebook have addressed the status of detained state counsellor and NLD leader Aung San Suu Kyi, [4] impending internet shutdowns, [5] bank fraud, [6] the likelihood of violent crackdowns by the military, [7] deepfake technology, [8] and the role of China's government in supporting the coup. [9] Some false rumors, such as those about Aung San Suu Kyi, have resulted in large public reactions before being dispelled. [10] Unintentional

misinformation that reflects poor digital literacy or a lack of available and trustworthy information has spread alongside propaganda and disinformation.

The state's censorship efforts had affected the diversity of online content produced by independent sources in the years prior to the coup. For example, in 2019 the military requested that the media refrain from saying "civil war" when referring to the country's internal conflicts. [11] In 2017, the government ordered that all media use the term "terrorist" instead of "insurgent" or "militant" when referring to Rohingya rebels. [12] Also in 2017, the British Broadcasting Corporation (BBC) announced that it would end its partnership with MNTV after the network repeatedly pulled BBC programs, apparently for using government-restricted words like "Rohingya," according to some analysts. [13] In June 2018, US-backed Radio Free Asia (RFA) canceled its partnership with the Democratic Voice of Burma after the government repeatedly attempted to censor the word "Rohingya" on its programs, which aired on state television. [14] RFA, however, reported that it would still cover Myanmar in other formats. [15]

The dominance of Facebook as the main channel for internet use in Myanmar has severely undermined diversity of information online, particularly since it has been blocked. The most-visited websites in Myanmar in 2020 were Google, YouTube, and Facebook. [16] However, a staggering 78 percent of users had never used an internet browser or app stores as of 2020, with most users accessing the internet via Facebook apps on their mobile phones. [17] The most popular Facebook pages were mostly run by media outlets, some of which were foreign. [18]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**2** / 6

TOP

Score Change: The score declined from 4 to 2 because the military erected extreme and varied obstacles to online mobilization in a bid to

quash anticoup protests, though users continued their attempts to mobilize using digital tools during parts of the coverage period.

The military has tried to significantly impede the people's ability to associate or assemble in opposition to its seizure of power. On the first day of the coup, the military shut down internet service to prevent the free flow of information. [1] The next day, the nationwide civil disobedience movement was launched by medical workers on Facebook. [2] As the protests and civil disobedience movement grew, the military ordered telecommunications companies to block Facebook and other communications platforms, and when users circumvented those blocks, the military instructed telecommunications companies to shut down the internet entirely for most people (see A3). [3]

Despite the restrictions, people continued to use online tools to organize and share information whenever possible. On February 22, a day of extensive protests, three local outlets broadcast 65 live video streams on Facebook. [4] Users have tried a range of tactics to circumvent the military's blocking efforts; VPNs and secure communications tools have become widespread. The maker of one secure communications app, Bridgify, reported that it was downloaded over a million times in Myanmar within the first two days after the coup. [5] The circumvention app Psiphon was downloaded by nearly two million users during the same period. [6] Users benefited from foreign counterparts' recommendations regarding applications that allowed them to chat anonymously or bypass censorship, as prodemocracy activists within the multinational grassroots protest movement known as the Milk Tea Alliance shared their knowledge. [7]

The three-fingered salute previously used in Thailand—a pillar of the Milk Tea Alliance—to signal opposition to authoritarian rule has become massively prevalent in Myanmar among supporters of the democratic movement, both online and offline. [8] In a related development, support for the rights of Rohingya people has increasingly become a feature of the anticoup protest movement, as evidenced by hundreds of thousands of users posting images of themselves wearing black and holding up the three-finger salute with the hashtag "#Black4Rohingya" in June 2021. [9]

TOP

The military has tried to disrupt users' ability to circumvent its digital controls. On March 30, one regional military government ordered telecommunications companies to disclose lists of subscribers in order to identify who still had internet access. [10] A long list of surveillance tools from vendors in countries including Canada, the United States, Sweden, and Israel has been published by activists reviewing government accounts (see C5). [11] The military has also reportedly submitted daily directives to telecommunications companies, each of which names hundreds of IP addresses to be blocked, in an attempt to end the viability of VPN services (see C4). [12]

The government also impeded people's ability to protest for digital rights prior to the coup. Online campaigning under the hashtag #StopInternetShutdownMM was combined with offline protests to call for an end to the service shutdowns in Rakhine and Chin States. [13] Eleven students and six activists were arrested in February and June 2020, respectively, for participating in peaceful offline protests against the restrictions. [14] One activist arrested in June was fined 30,000 kyats ($22.50) that September for hanging an antishutdown banner without permission. [15] Other forms of online protest—including a 2018 campaign in which many users changed their Facebook profile pictures to black spots to protest the imprisonment of two journalists, and a 2017 #SayNOto66d campaign aiming to decriminalize defamation—had also been prominent before the coup.

C. Violations of User Rights

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?	**0** / 6

TOP

Score Change: The score declined from 1 to 0 because the military's actions have effectively nullified the constitution and its limited protections for free expression.

By undertaking the February 2021 coup, the military effectively nullified the constitution, along with the limited protections for free expression that it offered. The junta claimed that the coup—carried out under the cover of a year-long state of emergency that the military said was necessary to address unverified claims of fraud in the November 2020 elections—was in line with its powers under the constitution. However, both the stated justification and the process itself were criticized by numerous civil society groups and legal organizations as being clearly unlawful. [1] Furthermore, legal experts have observed that many of the military's actions since the coup were unconstitutional, and that the rule of law has essentially collapsed. [2] Members of the Constitutional Tribunal, the one state body that might have held the authorities accountable to the constitution, were all replaced by the military on February 9, 2021. [3]

The constitution and other laws in Myanmar had largely failed to protect human rights online. The constitution, drafted by a previous 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. [4] It also provides specific—but highly limited—guarantees for citizens to "express and publish their convictions and opinions," [5] and to "freely develop literature, culture, arts, customs, and traditions," [6] 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." [7] The constitution includes no provisions directly relating to the internet or access to information, although Article 96 and Schedule 1 (8.m) grant the parliament authority to establish laws regulating the internet. In February 2019, the government established a joint parliamentary committee to recommend constitutional amendments to address access to the internet and information. [8] Later that year, a coalition of civil society organizations put forward their demands relating to freedom of expression. [9] The committee's final recommendations did not include any substantive changes to human rights or internet freedom in particular.

TOP

Fair trial rights are often violated in Myanmar's courts: the accused often have no effective representation, they receive limited access to court documents, and judges are inattentive during proceedings. [10] Trials concerning online activity commonly include significant procedural errors, technically unreliable evidence, and deep-seated judicial unwillingness to consult expert testimony. [11] In many cases, courts have been presented with easily forgeable printouts of digital content, or have ruled without testing the authenticity, reliability, or admissibility of evidence. [12]

Judicial independence is impeded by political interference. Under the constitution, judges were nominated by the president, and lawmakers could reject the choice only if it was clearly proven that the nominee did 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 undermine online media freedom. A 2018 amendment to the Broadcasting Law failed to clarify the country's transition from analog to digital broadcasting, which created an arbitrary process that could be misused by the government to control broadcasters and online media. [13] Also in 2018, the Myanmar Press Council, a once quasi-independent body that settled disputes involving the media, submitted to the government a proposed amendment of the 2014 News Media Law, which regulates digital media. Whether this proposal would have positively or negatively affected media freedom is unclear. [14] The draft of a right to information law first proposed in 2017 was preempted by new information-related laws and drafts. In December 2019, the National Records and Archives Law was adopted, limiting access to information and retaining secretive standards for government documents, including electronic documents, while further criminalizing the sharing of such material. [15]

C2 0-4 pts

TOP

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**0** / 4

Since the coup, the military has increased the number and harshness of laws criminalizing online activity.

The Telecommunications Law was drafted by a military-backed civilian government in 2013 with the support of the World Bank, [1] and it remains the primary framework for licensing telecommunications providers, including mobile service providers and ISPs. Although the law was welcomed by many stakeholders at the time as a sign of much-needed change, [2] the then government, led by the USDP, added a number of troubling provisions, including Article 66(d)—a vaguely worded measure that criminalizes a range of acts online, such as defamation—and Article 68, which criminalizes "communication, reception, sending, distribution, or sharing of incorrect information with dishonest intention." [3]

The law was amended in 2017 but with no discernible impact, according to civil society activists. [4] Civil society organizations launched a campaign for revision of this and other laws in the run-up to the 2020 general elections. [5] In December 2020, a civil society coalition launched a new push to amend Article 66(d) and the country's five other criminal defamation provisions, putting forward four reform options. [6]

The penal code can also be used to imprison internet users. Section 505 (a) criminalizes speech "with intent to cause, or which is likely to cause, any officer, soldier, sailor or airman, in the Army, Navy or Air Force to mutiny or otherwise disregard or fail in his duty as such." [7] Section 505 (b) outlaws speech "likely to cause fear or alarm in the public." [8] On February 14, 2021, the military unilaterally amended the penal code to broaden the scope of the crimes of high treason and sedition. [9] The amendments included vaguely worded provisions against knowingly spreading "false news," causing "fear," and the "disruption" of military or government officials. The section covering "false news" has been used to charge hundreds of journalists, human rights defenders, and digital activists (see C3). [10]

TOP

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. [11] The defamation provisions were amended in 2020 but are still used to prosecute individuals for online activity (see C3). [12] On February 10, 2021, the military suspended parts of the law, including its limited protections against surveillance and the interception of private messages. [13]

The military circulated a draft cybercrimes law to telecommunications providers on February 11, 2021 (see A3, C5, and C6). The draft was widely condemned, and more than 250 civil society organizations warned that it would give the military absolute control over the internet in Myanmar and extend military jurisdiction to foreign companies such as Facebook. [14] Much of the draft law circulated by the military was reportedly carried over from a draft created by the previous government but not shared widely. [15] In 2019, the government had commissioned consultants to assist in developing a such a law, [16] stating that the new framework would include provisions penalizing those who "insult the country and people and commit crimes over any communications network." [17] Human rights defenders have expressed concern that the proposed legislation, like other restrictive laws governing online activity in recent years, would be vague, overly broad, and used to punish a range of online behaviors. [18]

The draft cybercrimes law has not been publicly withdrawn, but following the widespread outcry, the military quickly amended the Electronic Transactions Law in February 2021, copying over many of the problematic provisions from the contentious draft. [19] These included new rules that could be used to criminalize the publication of "false information" or information that could damage foreign relations. [20] The USDP-led government had amended but failed to repeal the 2004 Electronic Transactions Law in 2013; it 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" information with those effects. The law was routinely used to criminalize internet activism during the previous period of military rule.

TOP

In response to the COVID-19 outbreak, the NLD-led government put forward a draft Prevention and Control of Communicable Diseases Bill in February 2020. The bill included a provision that imposed fines and a potential six-month prison term on health officials who disseminate certain health information during specified times if it could cause fear or panic. [21] Authorities claimed that the draft law sought to prevent public disorder and the spread of intentionally false information. The bill remained in draft form at the time of the coup.

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 ($3,800). [22] It was adopted alongside the Patent Law and the Industrial Design Law, which also include criminal sanctions for violations. [23] In May 2019, a copyright law that includes prison terms of up to three years for commercial copying without consent was adopted. [24] Each law applies to online content and could be used against users.

After a series of leaked draft laws criminalizing "hate speech" received significant criticism from civil society in 2017, the process of developing such a law was largely kept secret, and a bill had not yet been put before the parliament at the time of the coup. [25] The government claimed in 2017 that consultations with civil society regarding the bill had occurred, [26] but several well-known civil society organizations working on the issue refuted these assertions and had received no responses to their requests for meetings with the parliament. [27] The government in April 2020 issued a Directive on the Prevention of Incitement to Hatred and Violence, ordering officials to address the issue of hate speech. [28] The directive came in advance of a reporting deadline set by the International Court of Justice.

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	TOP **1** / 6

Internet users are frequently prosecuted in Myanmar's restrictive legal environment. Between the start of the coup and June 2021, 86 journalists and media workers had been charged under at least 10 laws, in many cases for their journalism published online. [1] The vast majority were awaiting sentencing at the end of the coverage period and had been held in pretrial detention. [2] The military has also targeted prominent social media users—including influencers, actors, singers, and food and beauty bloggers—by adding them to wanted lists that are broadcast nightly for those charged under Section 505A of the penal code (see C2). At least 60 people were on these lists as of early April. [3]

The Committee to Protect Journalists (CPJ) identified Myanmar as one of the world's worst jailers of journalists in a report published after the coverage period. [4] The organization listed at least 32 journalists in jail as of July 1, noting that the actual number was likely higher given that its sources feared repercussions for identifying detained colleagues. Though all but one of those listed had been placed behind bars during the coverage period, Democratic Voice of Burma reporter Min Nyo was the only journalist to receive a conviction by the end of that period. Min Nyo was sentenced to three years in prison in May 2021 under Section 505A of the penal code; he had been in pretrial detention since he was arrested while covering protests in March.

Other journalists detained under Section 505A include Nathan Maung and Han Thar Nyein, cofounders of the online news website Kamayut Media. They were detained during a March 2021 raid on the outlet's office, after which Maung reported being interrogated about the publication. The two also reported being tortured in detention (see C7); though Maung, a US journalist, was freed on June 15, Han Thar Nyein remained in prison as of the end of the month. [5] Four others on the CPJ list were handed two- or three-year prison sentences after the coverage period, in June 2021.

Some cases are clearly intended to silence the media's investigative journalism. In January 2021, the military filed a lawsuit against an editor and a journalist from the Rakhine-based Development Media Group under Article 66(d) of the Telecommunications Law after their outlet published a story about military corruption on its website and Facebook page. [6] The

TOP

group's editor in chief was already in hiding after being prosecuted under the Unlawful Associations Act for previous coverage.

Other cases in recent years have been aimed at punishing criticism that has gone viral online. In February 2020, Kay Khine Tun, Paing Phyo Min, and Su Yadanar Myint of the poetry troupe Peacock Generation were sentenced to six months in prison under Article 66(d) of the Telecommunications Law for sharing images of and live-streaming their performances satirizing the military on social media. [7] In December 2019, four other members of the group had also been sentenced to six months in prison under Article 66(d). [8] In June 2020, 25 members of Peacock Generation were called to a different court to face similar charges under Article 66(d). [9]

In addition to journalists and prominent social media figures, everyday users have had charges brought against them under various laws. High school student Maung Tin Chan was sentenced to five years' imprisonment in December 2020 for incitement under Article 33(b) of the Electronic Transactions Law, having published critical Facebook posts related to the conflict in Rakhine State. [10] In September of that year, the military brought a case against Thinzar Than Min for alleged defamation under Article 66(d) and alleged disinformation under Article 68(a) for a Facebook post in which she reported being pressured to support the military-backed USDP in the November general elections. She was convicted and sentenced to nine months in prison under Article 505(a) of the penal code in December 2020. [11]

From 2019 to 2020, there were more than 45 criminal cases under the Telecommunications Law and 21 cases under the Law Protecting the Privacy and Security of Citizens. Many plaintiffs in the cases were affiliated with the state, including public officials, NLD party officials, and military officers, while many of the accused were unaffiliated users, activists, and journalists. [12]

TOP

In May 2019, Reuters journalists Wa Lone and Kyaw Soe Oo were pardoned after being imprisoned for more than 500 days and convicted in September 2018 for reporting on the massacre of 10 Rohingya men and

boys. [13] The journalists had been sentenced to seven years in prison for violating the Official Secrets Act. [14] 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).

C4 0-4 pts

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

Score Change: The score declined from 3 to 2 because the military banned VPNs, limiting anonymous communication online.

Users' ability to communicate anonymously has been further restricted by the military since the coup. In March 2021, daily directives banned the use of VPNs, [1] though some orders barring VPN use emerged as early as February 4. [2] The Open Observatory of Network Interference (OONI) confirmed that multiple circumvention-tool websites were blocked at least once alongside their IP addresses in February 2021. [3] Although the blocking limited some people's ability to use circumvention tools, they continued to be used by the public. Civil society observers suggested that the impracticality of the VPN blocking was one of the reasons for the military's shift toward listing approved sites and services rather than attempting to update blocking lists. [4]

Anonymity has also been limited by the government's enforcement of SIM-card registration requirements, [5] whereby subscribers must provide their name, citizenship identification document, birth date, address, nationality, and gender, [6] and noncitizens must provide their passports. Some subscribers have reported being required by telecommunications companies to include further information beyond the bounds of the regulations, including their ethnicity. [7] Mytel reported in February 2020 that only 30 percent of subscribers had registered. [8] The MoTC announced that month that it had blocked over 6.5 million unregistered SIM cards. [9] The MoTC then ordered telecommunications providers to bar outgoing calls for millions of additional unregistered SIM cards, starting in April 2020. [10] At the end of June 2020, the cards were

TOP

reportedly deactivated, with the corresponding phone numbers deleted and subscriber money forfeited.

In March 2019, the government asked mobile service providers to limit each user to two SIM cards in order to protect "personal and national security." [11] It is unclear how this is being implemented by providers.

The government was working to establish biometric SIM-card registration prior to the coup. In November 2019, authorities released a tender to create a database that can store up to 70 million records of biometric data received from mobile-service registrations, [12] and the tender was closed in June 2020. [13] The government announced that month that it had requisitioned resources from the USF (see A2), which was intended to support mobile access for marginalized areas, to pay for the biometric database. [14] The database would include fingerprints and facial-recognition information. [15] It is unclear which company won the tender. The draft legal framework required to implement the plan, including data protection laws, had not been made public prior to the coup.

There are no clear restrictions on encryption in law, although vague provisions in the Telecommunications Law and the Electronic Transactions Law could be interpreted to restrict the practice.

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

Score Change: The score declined from 2 to 1 due to new evidence that authorities have obtained surveillance technology such as data extraction tools, as well as problematic legal changes including the suspension of limited privacy safeguards under the Law Protecting the Privacy and Security of Citizens and an amendment to the Electronic Transactions Law that increased government access to personal data. TOP

State surveillance grew more pervasive during the coverage period. Despite the fact that Article 357 of the constitution included protection for private communications, government surveillance was a serious concern

prior to the coup. After it seized power, the military circulated a draft cybercrimes law that would place all private data under its unchecked control. [1] The draft law requires service providers to store private data on servers designated by the military, and to make them accessible to military interception without any form of oversight (see C6). [2] Although the draft has not yet been enacted, the military unilaterally amended the Electronic Transactions Law in February 2021 by adding some of the same problematic provisions included in the draft. [3] For instance, the revised law grants the authorities broad powers to inspect any device on vague bases such as “misuse.” [4] The military has also effectively suspended some of the limited privacy protections afforded in the Law Protecting the Privacy and Security of Citizens, including its modest safeguards against warrantless surveillance and interception of private messages. [5]

Recent reports have confirmed the growing scope of the state’s surveillance efforts. A Reuters article from May 2021 described how former military officials had pressured providers in late 2020 to install interception technology that would enable the military to view texts and emails, listen to phone calls, and locate users without assistance or approval. [6]

New evidence of government purchases of hacking and extraction technology came to light in March 2021, when budget files obtained by Justice for Myanmar exposed acquisitions amounting to tens of millions of dollars since 2018, including tools from vendors based in Canada, the United States, Sweden, and Israel. [7] These included MacQuisition forensic software, which can extract data from Apple computers; MSAB Field units, which can extract even deleted content from mobile devices; and additional technology that has enabled security forces to determine the home addresses of online critics using their posts and the locations of their internet connections.

TOP

Earlier reports from 2018 indicated that the government had spent $4.8 million on surveillance technology, [8] which it allocated to the Social Media Monitoring Team (SMMT), [9] a body established under the MoTC following requests from the parliament in February of that year. [10] The

government refused to reveal from which country the equipment was purchased, citing security concerns. [11] One telecommunications company had warned that the government was creating a framework for direct interception of user data without proper safeguards. [12]

The NLD-led government argued that the SMMT was necessary to counter individuals causing "instability" online, including through hate speech and defamation. [13] Public statements by senior government officials in May 2018 specified that the SMMT's mandate focused narrowly on foreigners and foreign organizations suspected of causing unrest and threatening the country's sovereignty through interference. [14] 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 crisis and conflicts involving other ethnic minority groups in Myanmar, as well as the International Criminal Court and other international institutions pushing for accountability for the atrocities against the Rohingya. The SMMT was widely criticized by civil society organizations. [15] Little is known about the body's operations or whether there is any oversight. [16] Civil society activists suspect that the SMMT is now being used by the military to surveil those opposed to the coup. [17]

Since the coup, the police and military have reportedly seized the mobile phones of people they detain, and are thought to use the aforementioned extraction technology on such devices. The authorities are also believed to use drones and security cameras equipped with facial-recognition technology to surveil the public. [18]

The confiscation of phones—particularly from human rights defenders, activists, and journalists—also occurred prior to the coup. [19] The police reportedly demanded passwords for social media accounts and other applications from people accused of criminal activity, including in cases where the allegations were unrelated to social media use. [20] For example, shortly after Reuters journalists Wa Lone and Kyaw Soe Oo were arrested in 2017 (see C3), the police were accused of using Wa Lone's confiscated phone to send a WhatsApp message on his account.

TOP

[21] The police used the Israeli phone-breaching product known as Cellebrite to collect data from the journalists' smartphones. [22] 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 them. In 2019, FinSpy malware developed by Germany's Gamma Group was reported to be in operation in Myanmar. [23] It is unclear who purchased the spyware.

In 2018 the MoTC announced its intention to build a data center that would serve as a secure base for its planned e-government services in Naypyidaw, and in December of that year the ministry requested that the parliament approve a $95 million loan from South Korea to support the project. [24] The Mandalay regional government launched a data center in January 2019 to provide e-government services. [25] Concerns have been raised that these data centers will lack adequate privacy and security safeguards. [26]

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**1** / 6

Service providers are increasingly obliged to hand data over to the state without sufficient oversight or safeguards.

The Law Protecting the Privacy and Security of Citizens, passed in 2017 and partially suspended since the coup, [1] prohibits the interception of personal communications without a warrant, but it contains a vague exception allowing surveillance if permission is granted by the president or a government body. [2] 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. [3] Other privacy-related laws demanded by a range of private-sector and civil society stakeholders, including a robust data protection law, have not yet been introduced. [4]

TOP

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." [5] A provision stating that any interception should not "hurt the fundamental rights of citizens" is an inadequate safeguard against abuse. [6] The Telecommunications Law also grants the government the power to inspect the premises of telecommunications license holders and to require them to hand over documents—for the ill-defined purposes of defending the "security of the state" or "the benefit of the people"—without safeguards for individuals' privacy and other human rights. [7] A 2018 amendment to the Narcotic Drugs and Psychotropic Substances Law included a new provision requiring telecommunications providers to disclose user information without due process. [8] There are no requirements for judicial review.

Civil society activists have raised concerns that the opaque mass directives being issued to service providers by the military since the coup include orders for widespread interception (see A4, B1, and B3). [9] The draft cybercrimes law would also require service providers to store data on servers designated by and fully accessible to the military (see C5). There is little room for providers to push back against the military's directives, though in at least one instance they did so effectively. On March 30, one regional military official ordered telecommunications companies to disclose lists of subscribers in order to identify who still had internet access; [10] the companies reportedly appealed successfully to the military on the grounds that the move would violate their license requirements.

The largest state-owned telecommunications provider, MPT, has not publicized the number of requests for data it receives from authorities. Telenor announced that in 2019 it received 188 requests for communications data, about triple the number received in 2018, and complied with 88. [11] Mytel stated that it had received over 100 requests from the police for user data during 2019. [12] Both claimed that the majority of requests were related to human trafficking, missing people, and drugs. [13] The content of these requests is unclear. One major provider stated in 2018 that it initially required three documents before

TOP

disclosing information, including a letter from a senior police officer and a letter from the PTD, but it has in practice dropped the requirement for a judicial warrant. [14]

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?	**0** / 5

Score Change: The score declined from 2 to 0 due to reports of widespread physical violence in reprisal for online activity, including torture in detention.

Since the coup, the military has forcibly disappeared and publicly beaten influential social media figures, and physical and mental torture of those in detention has become widespread. [1] The junta has threatened deadly repercussions for those who support or participate in the anticoup protests, the civil disobedience movement, or a committee representing political forces opposed to the coup. [2] The military has also actively searched for people who use the internet to support these endeavors. [3]

At least 23 journalists, many of whom produced online content, have been shot or severely beaten by the military. [4] For example, CPJ reported that Nathan Maung and Han Thar Nyein, the cofounders of the online news website Kamayut Media, were beaten in detention after being arrested in March 2021. In an interview with CPJ, Maung alleged that Han Thar Nyein was burned with lit cigarettes, made to kneel on ice, and subjected to an attempted sexual assault by soldiers. [5] The soldiers also demanded that he hand over his iPhone password. Han Thar Nyein remained in detention as of June 2021 (see C3). [6]

The military leadership has also leveled threats against soldiers over online activity, for instance if they use Facebook via a VPN. [7] Officials at military checkpoints set up between major cities reportedly confiscate mobile phones, which are then examined to assess the owner's Facebook activity. [8] Civil society groups have established a mechanism for closing down the social media accounts of detained individuals to prevent them

TOP

from self-incriminating or incriminating others. [9] Renowned digital rights activists have also been in hiding since the coup; their organizations have effectively been shut down, and they believe they are at risk of death if found or detained by authorities. [10]

Online journalists, human rights defenders, and political activists reported intimidation and threats of violence prior to the coup, although to a significantly lesser degree. In one opinion survey published in May 2020, most journalists reported that they believed violence against members of the media had increased compared with the previous year. [11]

Journalists reporting on the Rohingya crisis or covering the Rakhine State and Shan State conflicts have faced special risks of violence in recent years. [12] During the trial of Reuters journalists Wa Lone and Kyaw Soe Oo, defense lawyers informed the court that the journalists were tortured in detention. [13] 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 interrogated. [14] He also said that authorities covered his head with a black hood.

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 issue they focus on in their work. Pro-Rohingya and peace activists report high levels of intimidation via direct and indirect messages and comments online. [15] Allegations of torture have also been made against police, prison guards, and border guards by student activists, [16] monks, [17] and others. [18] Women who are high-profile users or human rights defenders report regular gender-based intimidation and threats of violence. [19] 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 extortion attempts.

TOP

A significant number of internet users have reported experiencing cyberbullying, particularly those who belong to marginalized groups,

including young women, members of religious minorities, and the LGBT+ community. [20]

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 services are subjected to technical attacks in Myanmar.

Human rights defenders, journalists, and political activists continue to report regular, often weekly, remote attempts to hack their email and Facebook accounts, including during the postcoup period. [1] Digital activists in Myanmar note that Google regularly warns them of "government-backed attackers" attempting to hack their Google accounts. [2] Pro-Rohingya and Muslim activists are among those who report frequent hacking attempts. [3] Police use sophisticated technology to break into the devices of journalists, including Reuters reporters Wa Lone and Kyaw Soe Oo in 2017. [4] Advanced spyware has been identified in Myanmar, [5] and human rights defenders, journalists, and political activists have reported the presence of spyware on their mobile phones (see C5). [6]

Since the coup, several government websites, including those of the central bank and state television stations, have been hacked and defaced with antimilitary messages. [7] In 2017, the websites of the Ministry of Culture, the central bank, and Maubin University, in addition to some private webpages, were hacked and populated with messages reading "Stop Killing Muslims." [8] The hacks were allegedly carried out by Turkish activists to highlight atrocities against the Rohingya. [9]

Microsoft has raised concerns about the large number of computers and devices in Myanmar that are infected by viruses and malware. [10] Kaspersky reported in 2020 that Myanmar comes in second globally for the highest rates of virus infections, with 60 percent of computers and removable media compromised. [11] Browser modifiers are twice more

TOP

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 by the malware worm Win/Macoute; the worm spreads through USB drives, which are very common in Myanmar, and communicates the drive's contents to a remote host. [12]

On Myanmar

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

See More ›

Country Facts

Global Freedom Score

28 /100 **Not Free**

Internet Freedom Score

17 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

TOP

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

TOP