



Freedom on the Net 2021

Egypt

NOT FREE

26

/100

A. <u>Obstacles to Access</u>	12 /25
B. <u>Limits on Content</u>	10 /35
C. <u>Violations of User Rights</u>	4 /40

LAST YEAR'S SCORE & STATUS

26 /100 Not Free

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



Overview

Internet freedom and the rights of internet users continued to deteriorate during the coverage period. Authorities launched a targeted campaign

against women social media influencers and a number of TikTok users received prison sentences. Censorship continued to negatively impact freedom of speech, as authorities utilized Sandvine technology to block hundreds of websites and surveil internet users. The Supreme Council for Media Regulation (SCMR) continued to manipulate the media landscape by blocking independent news sites, forcing publishers to remove online content deemed critical of the government, and issuing reporting guidelines. Criminal penalties, harassment, and surveillance have contributed to high levels of self-censorship among Egyptian internet users, particularly independent media outlets and government critics. Authorities continued their practice of “recycling” detainees, and some journalists, activists, and bloggers who were imprisoned on earlier charges were resentenced during the coverage period.

President Abdel Fattah al-Sisi, who first took power in a 2013 coup, has governed Egypt in an increasingly authoritarian manner. Meaningful political opposition is virtually nonexistent, as expressions of dissent can draw criminal prosecution and imprisonment. Civil liberties, including press freedom and freedom of assembly, are tightly restricted. Security forces engage in human rights abuses with impunity. Discrimination against women, LGBT+ people, and other groups remain serious problems, as does a high rate of domestic violence.

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

- In October 2020, authorities blocked Telegram on three networks. Authorities failed to provide an explanation for the blocking (see A3 and B3).
- In October 2020, it was revealed that Egyptian authorities used Sandvine devices to block 600 websites and surveil internet users through deep packet inspection (DPI) technology (see B1 and C5).
- Progovernment bots attempted to manipulate the online space. During the coverage period, Facebook and Twitter removed

hundreds of accounts due to “inauthentic coordinated behavior” (see B5).

- Since April 2020, the Egyptian authorities have targeted women TikTok influencers. During the coverage period, at least three women received prison sentences for “violating family values and principles” on social media (see B8, C3, and C7).
- In August 2020, prominent human rights defender and director of the Cairo Institute for Human Rights Studies (CIHRS), Bahey eldin Hassan, received a 15-year in absentia prison sentence, the longest imposed on a human rights defender in Egypt (see C3).
- In September 2020, Amnesty International’s Security Lab reported new examples of FinSpy being used against Windows and Android devices, along with previously unknown versions targeting Linux and macOS computers (see C5).
- President Sisi ratified a data-protection law in July 2020. While it is the first legal safeguard of its kind in Egypt, some clauses may negatively impact individual user privacy (see C6).

A. Obstacles to Access

A1 0-6 pts

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

4 / 6

Score Change: The score improved from 3 to 4 because internet users in Egypt experienced faster internet speeds, according to some measurement sources.

The Egyptian government has made efforts to improve the information and communication technology (ICT) infrastructure and increase the number of internet users, though internet connections continue to suffer from poor quality and low speeds. According to the *Information and Communication Technology Indicators Bulletin*, a report issued by the Ministry of Communications and Information Technology (MCIT), internet penetration stood at 57.3 percent in September 2020. The mobile-phone

penetration rate was 94.1 percent, amounting to more than 95.4 million subscriptions. ¹

Egyptians are increasingly using mobile services to access the internet. According to a 2020 MCIT report, there were 48.5 million internet users, ² but only 8.45 million asymmetric digital subscriber line (ADSL) subscriptions, which use fixed-line infrastructure. By contrast, there were 50.5 million mobile internet users. ³ Egypt scored 55.7 out of a possible 100 points on the 2019 GSMA Mobile Connectivity Index, which measures the performance of 170 countries on key mobile internet indicators. ⁴ In a June 2021 Speedtest report, Egypt ranked 97th out of 134 countries for mobile internet speeds and 91st out of 176 countries for fixed-line broadband speeds. ⁵ Egypt also ranked 84th out of 134 countries in the 2020 Network Readiness Index, receiving its highest score in the governance pillar (trust, regulation, and inclusion). ⁶

In response to the COVID-19 crisis and the social distancing measures adopted during the first half of 2020, the MCIT instructed internet service providers (ISPs) to raise the internet bandwidth of fixed-line broadband services by 20 percent without extra charge. Some ISPs also offered temporary discounts. ⁷ In June 2020, the MCIT announced a \$1.6 billion investment aimed at improving the ICT infrastructure and increasing internet speeds from 5.7 megabits per second (Mbps) to 20 Mbps by the end of 2020, and to 40 Mbps in 2021. The government also plans to spend \$400 million to connect two million homes to the internet. ⁸

The National Telecommunication Regulatory Authority (NTRA) has led reforms to upgrade the telecommunications infrastructure and increase internet speeds by installing fiber-optic cables. In 2016, it auctioned fourth-generation (4G) mobile service frequencies to all mobile providers ⁹ which increased data usage and allowed operators to improve service offerings. ¹⁰ During a Cairo ICT conference in November 2018, the NTRA announced that more advanced fifth-generation (5G) mobile networks were expected to be launched in Egypt by 2020. ¹¹ In February 2019, Telecom Egypt partnered with Nokia to deploy 5G technology and test it in the Egyptian market. ¹² In mid-2018, the MCIT announced plans to improve fixed-line connection speeds by switching from copper to fiber-

optic cables. According to tests undertaken in recent years by Speedtest, Akamai Technologies, and OpenSignal, the quality of fixed-line connections in Egypt is relatively poor. ¹³ In July 2019, the ICT minister launched the NTRA's National Centre for ICT Services Quality Control and Monitoring to assess the quality of telecommunications and internet services provided in Egypt. ¹⁴

In February 2021, the Roland Berger Digital Inclusion Index ranked Egypt as one of the top 10 improvers of the 82 countries it assessed during its 2020 reporting period, attributing its score increase to infrastructure, availability, and coverage improvements. The country's accessibility score increased by 13 points over its 2017 score, from 37 to 50. 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
---	---------------------

Broadband internet connections are relatively affordable.

A monthly 140 GB mobile package costs 120 Egyptian pounds (\$7.65). ¹ While state-owned ISP Telecom Egypt continues to dominate the sector, increased competition among mobile providers has caused a decrease in broadband prices. However, in September 2017, prices rose due to the implementation of a 14 percent value-added tax (VAT) on ADSL internet.

² Nonetheless, according to Cable, a London-based broadband comparison website, Egypt ranked ninth out of 195 countries on consumer broadband prices. In July 2020, Egypt was reported as one of the cheapest countries in the world for broadband packages, with an average price of \$17.83. ³ The Alliance for Affordable Internet's Affordability Report 2020 ranked Egypt 36th out of 72 countries in its internet affordability index. ⁴

The distribution of fixed-line internet access varies across different parts of the country. In September 2020, 36 percent of the country's ADSL subscriptions were in greater Cairo, 34 percent were in the Nile Delta region, 14 percent were in Upper Egypt, 10 percent were in Alexandria

and Matrouh, and 6 percent were in the Sinai, Red Sea, and Suez Canal areas. ⁵

Internet penetration is hindered by digital illiteracy, among other factors. The Economist Intelligence Unit's Inclusive Internet Index 2021 ranked Egypt 73rd out of 120 countries due to "low rates of usage and literacy."

⁶ In 2015, Facebook zero-rating services were provided by Emirati telecommunications firm Etisalat for two months, during which time three million internet users gained free access to the internet. While a government official claimed that the offer's permit was scheduled to expire in December 2015, the service's suspension was shortly before the fifth anniversary of the 2011 revolution, which had been driven in large part by organizing on social media. ⁷ Reuters reported that the zero-rating services were suspended because Facebook had refused to comply with a government request to help conduct surveillance. ⁸ During the COVID-19 pandemic, some ISPs offered discounts on internet packages. ⁹

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	3 / 6
---	--------------

The government has considerable control over internet infrastructure and has restricted connectivity.

Article 67 of the Telecommunication Regulation Law provides Egyptian authorities with the power to commandeer telecommunication services and networks of any operator or service provider and "call operation and maintenance employees of such services and networks in case of natural or environmental disasters or during declared periods of general mobilization in accordance with the provisions of Law No. 87 of 1960 or any other cases concerning national security." This means that the NTRA, alongside the military and national security agencies, is entitled by law to set the operational plan for the deployment of telecommunication networks during cases provided in Article 67. ¹

The government has centralized the internet infrastructure and fiber-optic cables to create highly controllable choke points. ² In addition, virtually all of Egypt's telecommunications infrastructure is property of Telecom Egypt. This arrangement facilitates authorities' ability to suspend internet access or decrease speeds, as was the case during the 2011 revolution.

³ In February 2019, Prime Minister Mostafa Madbouly issued Decree 242, which put the telecommunications infrastructure under the ownership of the National Service Projects Organization, which is run by the Ministry of Defense—further consolidating the state's hold on telecommunications in Egypt. ⁴

Voice over Internet Protocol (VoIP) services have been intermittently blocked on mobile networks. Disruptions to Facebook Messenger and Skype were reported during the September 2019 protests (see B1). ⁵ Interruptions of VoIP services were further reported amid the COVID-19 crisis, which hindered the capacity of Egyptians to check on their family and friends living abroad during times of social distancing. In response, the Office of the United Nations High Commissioner for Human Rights (OHCHR) called on the Egyptian government to work with civil society and the press rather than imposing restrictions on social media. ⁶

In October 2020, Telegram was reportedly blocked for customers of mobile service providers We, Vodafone Egypt, and Orange Egypt after authorities blocked access to the service's IP addresses. ⁷ The NTRA provided no justification for these disruptions. In April 2017, users experienced disruptions when attempting to make voice calls via applications like WhatsApp, FaceTime, Viber, Skype, and Facebook Messenger. ⁸ The disruptions may have been linked to the announcement of a three-month state of emergency after a terrorist attack killed dozens of people at a church on Palm Sunday. ⁹ The NTRA denied that VoIP calls had been restricted. ¹⁰ VoIP services had previously been blocked in October 2015, though in that case mobile service providers confirmed that the blocking had been requested by the NTRA. ¹¹ Periodic blockages of VoIP traffic over mobile networks were documented as early as 2010, ¹² but debate surrounding VoIP intensified in June 2013 after the NTRA announced the establishment of a committee to "monitor" communications on WhatsApp and Viber, pending

a potential decision to block or restrict them. The NTRA cited an economic rationale, noting that the free services had a negative impact on traditional telecommunications companies. ¹³ Making international calls over VoIP networks is technically illegal under Article 72 of the 2003 Telecommunication Regulation Law. ¹⁴

In December 2018, signal jamming was reported by international journalists visiting North Sinai as part of a state-regulated media tour meant to promote a “return to normalcy” in the wake of a government counterterrorism campaign. ¹⁵ In April 2019, communications disruptions were reported on social media following attacks by the Islamic State (IS) militant group in the Sinai city of Sheikh Zuweid’s central market. ¹⁶ Security forces reportedly shut down the internet and other communications networks for several hours as a result of the attack, which killed five civilians. ¹⁷

A4 0-6 pts

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

3 / 6

The Egyptian ICT market is dominated by a small number of companies, creating obstacles to competition and innovation.

Three companies largely control the mobile phone market. Vodafone Egypt enjoys the greatest market share, with 40.5 percent, while Orange Egypt has 33 percent. The latter, formerly known as Mobinil, underwent rebranding in 2016 and is now 99 percent owned by its French parent company. ¹ Etisalat Misr, with a 24 percent market share, is 66 percent owned by Etisalat, which has strong ties to the United Arab Emirates. ² In 2017, state-owned Telecom Egypt officially launched We, ³ the country’s fourth mobile network. Telecom Egypt also owns about 45 percent of Vodafone Egypt.

In January 2020, Vodafone announced the potential sale of 55 percent of their holdings in Vodafone Egypt to the Saudi Telecom Company (STC).

⁴ In response, the NTRA issued a press release highlighting that the

acquisition required its approval in order to safeguard the rights of users to telecommunication services. ⁵ The Financial Regulatory Authority (FRA), meanwhile, noted that the proposed sale requires a mandatory tender according to capital market legislation, Law No. 95 of 1992. ⁶ Additionally, Telecom Egypt declared that it would assess possible investment options and opportunities should the transaction come into force. Some experts speculated that Telecom Egypt could sell its stake for cash, as the company has accumulated over 15 billion Egyptian pounds (\$956 million) of debt since the launch of its mobile network. ⁷

In 2016, Etisalat Misr obtained a license to offer fixed-line services via Telecom Egypt's infrastructure. In 2017, Orange Egypt announced that it would also provide fixed-line services. In 2018, Vodafone began testing its fixed-line network. Nonetheless, Vodafone's decision on offering fixed-line services remained pending, as the segment is not considered particularly lucrative. In a 2020 report, the Oxford Business Group reported that none of the companies launched fixed-line services. ⁸

Vodafone and Orange launched 4G services in 2017 after receiving access to the frequencies from the government. We was the first mobile service provider to acquire a 4G license in 2016; the other three faced delays due to their refusal to meet NTRA criteria, including paying half of the license fee in US dollars. ⁹ In receiving the license for We, Telecom Egypt promised to sell its Vodafone shares within a year, but did not do so. ¹⁰

Telecom Egypt, under the banner TE Data, controls 75 percent of the ADSL market. Egypt's other main ISPs, also known as Class A ISPs, are Etisalat Egypt, Noor, and Vodafone Data. These companies lease lines from TE Data and resell bandwidth to smaller ISPs. ¹¹

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

Telecommunications services and ISPs are regulated by the NTRA under the 2003 Telecommunication Regulation Law, which does not guarantee the NTRA's independence. ¹

The authority is subordinated to the MCIT, and the members of its board are selected by the prime minister, who also determines their salaries. ² The NTRA board is chaired by the ICT minister and includes representatives from the Ministries of Defense, Finance, and Interior; the National Security Council; the presidency; and trade unions, among others. ³ Officially, the NTRA is responsible for ensuring a competitive market environment, managing the frequency spectrum, setting industry standards, and overseeing interconnection agreements. ⁴ In addition, it aims to enhance and integrate advanced telecommunications and broadband technologies. ⁵

The NTRA played a significant role in the five-day shutdown of internet and mobile services during the 2011 revolution. According to a judgment by an administrative court, the authority participated in all stages of the shutdown and represented the MCIT in this operation. It also worked with telecommunications companies to follow the Interior Ministry's decree calling for the shutdown; in the same judgment, the decree was ruled an infringement on the right to communicate, among other rights. ⁶

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
--	---------------------

The state continued to block news websites during the coverage period as part of a wider crackdown on freedom of expression and civil society activism.

In November 2020, IFEX reported that at least 600 websites were blocked by the authorities since May 2017, including 394 virtual private network

(VPN) and proxy providers and 116 news sites. ¹ While some of these websites were blocked for a limited period of time, others remained blocked throughout the coverage period.

During the coverage period, it was reported that the Egyptian government had used Sandvine's technology to block hundreds of websites, including 100 independent news and media websites. ² Authorities deployed Sandvine's equipment to censor the internet and record information about internet users' website-browsing histories (see C5). For example, the popular citizen news platform Al-Manassa was blocked using this technology. ³ According to IFEX, "Sandvine has a recorded history of facilitating human rights violations related to the production and selling of internet surveillance and censorship devices." ⁴

Many international and local news sites are blocked, some of which have been blocked since the beginning of 2017. Blocked sites include Huffington Post Arabic, financial newspaper *Al-Borsa*, and the entire online publishing platform Medium, where blocked news outlet *Mada Masr* had reposted its content. Websites run by Human Rights Watch (HRW), Reporters Without Borders (RSF), the April 6 Youth Movement (which was active in the 2011 revolution), and jailed democracy activist Alaa Abdel Fattah are also inaccessible.

In January 2021, an unidentified number of newspapers and news sites were referred for investigation by the SCMR, which claimed that it received complaints from the public regarding the "reputation and honor of ordinary citizens." In its statement, the SCMR reported that the outlets may have published "unethical content." ⁵

After the endorsement of the media regulations law in 2018 (see B3), a number of websites were blocked by the SCMR. In April 2020, the SCMR blocked the electronic and paper editions of privately-owned newspaper *Al-Masry al-Youm*. Additionally, the SCMR enforced a number of sanctions on the journal, including financial penalties, a disciplinary investigation by the Syndicate of Journalists, and a criminal investigation. While the SCMR's decision did not refer to any legal provisions to justify

its measures, it was reportedly prompted by a series of articles on Sinai published by newspaper owner Salah Diab under a pseudonym. ⁶

In May 2020, the SCMR banned journalists and writers working for newspapers and websites from using pseudonyms without prior written consent. Those seeking to write under a pseudonym are required to identify their reason in their requests. ⁷

In June 2020, the SCMR censored print and online media outlets from covering the Grand Ethiopian Renaissance Dam, COVID-19, and conflicts in Libya and the Sinai Peninsula. The SCMR confirmed the censorship measures, stating “the need for all media and social media sites,” to publish official data when “broadcasting information regarding Libya, the Renaissance Dam, and the military operations in Sinai against terrorism.” ⁸

In March 2019, the SCMR fined newspaper *Al-Mashhad* 50,000 Egyptian pounds (\$3,100) and instituted a six-month website block after it allegedly defamed media figures by publishing inappropriate photographs, ⁹ representing the first case of enforcement of the 2018 media regulation law. In April 2019, after *Al-Mashhad* appealed, the SCMR reduced the blocking duration to one month, though the site remained blocked for longer. ¹⁰

In December 2018, five sites owned by MO4 were blocked for lacking licenses. Moreover, the SCMR determined that an article published by MO4’s online magazine, *Al-Fasla*, had been an “unjustified insult to the Egyptian passport” (see B6), and that another outlet, *CairoScene*, published “indecent pictures and pornographic expressions.” ¹¹ After it was blocked, sports website *Ibarina* reported in January 2019 that a high-profile sports figure sought to block the MO4 sites in response to coverage of his intention to buy an Egyptian media group. ¹²

In May 2019, at least three cases were submitted to the Administrative Court of the State Council in an effort to identify the state bodies that ordered widespread blocking. In one instance, a committee responsible for the custody and administration of funds seized from the banned

Muslim Brotherhood issued a public blocking order, accounting for just 33 websites. ¹³

In April 2019, URL-shortening service Bitly, which is often used by online journalists and bloggers, was blocked for 12 hours by several providers, including Telecom Egypt and Etisalat. While a reason was not provided, it affected nearly 40 billion URLs. ¹⁴

Monitoring group NetBlocks found that more than 34,000 websites were blocked ahead of the April 2019 constitutional referendum in an apparent bid to suppress opposition to the amendments, which were adopted in a deeply flawed vote. Among other changes, the amendments allowed President Sisi to seek reelection through 2030, granted him more power over the judiciary, and reinforced the role of the military in politics. While Batel, which collected signatures in opposition to the amendments, was blocked, other sites with no clear connection to the referendum were also affected. ¹⁵ NetBlocks theorized that these sites, which shared a hosting IP range, were affected due to “collateral damage.” ¹⁶ Batel unsuccessfully attempted to remain accessible via other domains. ¹⁷

Reports of 11 messaging apps, including Wickr, Signal, and Wire, being blocked or restricted by authorities surfaced in September 2019. ¹⁸

NetBlocks reported disruptions to Facebook Messenger, Twitter, Skype, the British Broadcasting Corporation (BBC), and other news sites in the wake of antigovernment protests (see A3 and B8). ¹⁹ The SCMR’s head stated that the blockings were “likely” due to “inaccurate” coverage of the protests. ²⁰ Security experts were concerned that the “intermittent blocking” could be a test for a further complete blockage. ²¹

Service providers are sometimes further compelled to block websites during major political and national events. Websites were blocked during the COVID-19 pandemic; in April 2020, Masaar reported that several websites covering the pandemic were blocked on several service providers. ²²

During the pandemic, the SCMR warned 16 news sites and social media accounts, advising them against disseminating purportedly false coronavirus-related news in Tanta City and instructing them to use official

figures (see B5). ²³ The SCMR blocked or limited access to several websites for disseminating purportedly false news. In March 2020, the websites of Huna Aden and *Al-Gomhoria al-Youm* received six-month blocks, although it is unclear whether the blocking was carried out. Additionally, six social media accounts were blocked for “inciting violation of the preventive measures taken by the state” to fight the pandemic. ²⁴ The SCMR also issued blocks against news sites in April and May. ²⁵

Egyptian authorities also blocked alternative domains of websites that commented on the coronavirus in a way that did not confirm to official information. ²⁶ In April 2020, Darb, a news outlet run by the opposition Socialist Popular Movement Party, was blocked a month after its launch. Darb had published calls for the release of prisoners of conscience during the pandemic. ²⁷

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

In recent years, the government has removed objectionable content from certain outlets. In August 2019, an article on poverty in Egypt by professor Mostafa El-Said was banned in the *Al-Shorouk* newspaper. The reason for the ban was not clear; the article relied on income and expenditure data published by the Central Agency for Public Mobilization and Statistics. El-Said announced via his Facebook account that the outlet did not impose the ban. ¹

Other tactics have been used by nonstate actors to control the digital space. Private citizens can lodge legal complaints against the “violation of public morality” on social media, which allows authorities to censor online content, curtail freedom of expression online, and clamp down on internet users. During the reporting period, authorities launched a systematic crackdown on female TikTok users (see B8 and C3). ² Moreover,

proregime lawyers at times file lawsuits against social media content published by prominent opposition figures to rein in criticism. ³

News outlets regularly remove articles from their own websites. In May 2018, the Arabic website of Russian state broadcaster RT was pressured to remove an online poll it had posted regarding the disputed territories of Halayeb and Shalateen on the Egyptian-Sudanese border. The poll had drawn formal rebukes from the State Information Service (SIS) and the Ministry of Foreign Affairs and triggered the cancellation of an interview with the foreign minister. ⁴

According to Twitter’s transparency report, the Egyptian government did not submit any content removal requests but submitted one request for account information between January and June 2019. ⁵ Facebook disclosed one legal-process request and one emergency-disclosure request during its July–December 2020 reporting period. ⁶

Shortly before the September 2019 protests, the SCMR published an article under the title “Blocking and fines are the penalty for spreading rumours in the media” to reiterate Article 17 of the SCMR’s Sanctions Regulations, which provides penalties for spreading false news or rumors or inciting violation of the law. The sanctions vary from a penalty of up to 250,000 Egyptian pounds (\$15,900) to “preventing the publication or the broadcast or blocking the page or the program or the website for a specific period or permanently.” ⁷

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

The legal framework that regulates the digital space includes restrictions that are neither necessary nor proportionate, and largely lack transparency.

In May 2018, the Supreme Administrative Court ruled on an appeal of a 2013 case centered on a YouTube video that was deemed to have

denigrated the prophet Muhammad. The final ruling ordered regulators to block YouTube for a month, ¹ and government agencies and the NTRA were authorized to block websites on national security grounds. ² The decision limited the ability of administrative courts to restrict executive orders for online censorship and facilitated new legislation granting judicial and executive bodies the right to block websites. ³

In August 2018, a few months after the ruling, President Sisi signed a law to combat cybercrime and a law on media regulation, respectively. ⁴ The cybercrime law, Law No. 175 of 2018 (see C2), allows state authorities to block websites without a judicial order on national security or economic grounds, which are vaguely defined. Personnel at service providers that do not respond swiftly to blocking decisions could face prison and fines.

⁵ The government claimed that the law was meant to combat online theft and hacking. ⁶ The media regulations law, Law No. 180 of 2018 (see B6 and C2), requires that news sites obtain an SCMR license. However, whether blocked websites are able to apply for one, and whether they would remain blocked after obtaining one, is unclear. ⁷ In November 2018, blocked news site Katib closed after the SCMR stated it would not necessarily be unblocked even with a license. ⁸ In March 2019, officials published the SCMR's list of sanctions, which included potential penalties for violations of the media-regulation law such as suspensions, fines, and other disciplinary actions. ⁹

Additionally, the criminal code includes provisions regarding the dissemination of “blasphemous or defamatory material” which could be used to legally compel service providers to block such materials. ¹⁰ The broadly worded 2015 antiterrorism law allows authorities to block content or websites that promote terrorism. ¹¹

In March 2018, the ICT minister stated that the government was working to expand its social media influence by establishing an “Egyptian Facebook.” He reasoned that Facebook and Google, which are used by millions of Egyptians, were making millions of untaxed dollars from advertisements (see B6). ¹² A local Facebook alternative, which had yet to be created as of May 2019, would also be more vulnerable to state coercion.

After imposing a tight grip on traditional media, the Egyptian authorities have also closely monitored social media platforms. According to a July 2019 report by the Arabic Network for Human Rights Information (ANHRI), Facebook is the website that is most often monitored by the government. The ANHRI called Facebook users the “most prosecuted social media users in Egypt (see C3).” ¹³

Authorities have additionally censored and blocked online content and many websites opaquely, preventing defendants from understanding the reason for such procedures taken against them (see B1 and B6). In October 2020, three service providers blocked access to Telegram, with the government providing no justification. ¹⁴

In December 2019, the parliament approved the establishment of a State Ministry of Information, which Sisi approved in January 2020. The ministry will coordinate efforts with media regulatory bodies and state authorities. The president further commissioned the new minister to set “a professional and disciplined media capable of standing up to foreign hostile media campaigns targeting Egypt in the form of malicious rumours, TV reports, and social media attacks.” ¹⁵ The constitution does not refer to this new entity, however, and its establishment is at odds with constitutional provisions on the media regulator’s independence. ¹⁶

In May 2020, the Egyptian Public Prosecution published a statement which elucidates its role in enforcing the Cybercrime Law. It called upon citizens to “protect Egypt’s cyber borders” which necessitates “full deterrence and protection” to overcome “a phenomenon abused by forces of evil” seeking to “destroy our society, demolish its values and principles and steal its innocence and purity... to push its youth and adults to the brink of destruction.” ¹⁷

B4 0-4 pts

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

The rising number of arrests for social media posts has had a chilling effect on online speech. Online journalists are often reluctant to publish on sensitive topics, including sectarian tensions, sexuality, the Muslim Brotherhood, political detainees, military operations in the Sinai, and the military's outsized role in the national economy.

A provision in the 2015 antiterrorism law criminalizes the publication of information regarding militant attacks that contradicts official government statements, prescribing up to two years' imprisonment for violations. ¹ The media regulation law approved in August 2018 made the publication of false news, as defined by the government, a criminal offense (see C2). Also during 2018, the SCMR established a committee tasked with monitoring social media for any important trends or prevalent ideas or topics being discussed, which could further encourage self-censorship. ² To this aim, Cairo has further deployed advanced censorship and surveillance technologies to intimidate citizens and force them to self-censor, so as to curtail political opposition on digital platforms. ³

Self-censorship is prompted both by the government and by members of the public. In July 2020, a gay man was harassed on Facebook for his sexual orientation, and was later assaulted offline. Prior to this, the man had posted a TikTok video that included a rainbow flag. The video was uploaded on Facebook without his permission, and he temporarily closed his account after receiving intimidating messages and death threats (see C7). ⁴

A study published by the Association for Freedom of Thought and Expression (AFTE) in June 2020 found that increased censorship measures since 2017 have encouraged self-censorship. Specifically, news outlets refrain from publishing content critical of the government for fear of website blocks, or of further retaliation if they are already blocked. The study demonstrates how blocking websites has adversely impacted the online content produced in terms of quantity and quality. ⁵

Registering a web address using Egypt's .eg domain requires the submission of personal data and copies of the applicant's national

identification document (see C4), which may inhibit local sites from publishing criticism of the government.

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	1 / 4
---	--------------

Online news outlets are controlled for the purpose of suppressing dissent and quelling free expression. A variety of laws are used to reinforce this control (see C2). Journalists and bloggers face intimidation and smear campaigns from progovernment forces, online and in the news media (see C7).

The media landscape is dominated by the online versions of state-owned newspapers or outlets that are backed by government-connected businessmen. ¹ In March 2018, following a BBC report on human rights violations in Egypt, the public prosecutor launched a hotline for reporting purportedly false news. Individuals can use text messages or WhatsApp to register complaints against media outlets and social media for content that could threaten national security. ²

In September 2019, the SIS called upon international media correspondents to comply with international professional standards when covering news from Egypt. According to the SIS, this means social media outlets should not be considered news sources, “as these sources have an uncontrollable and chaotic nature with the presence of many fake accounts and fabrications.” The SIS further stated that “in developed nations such sources are not allowed to be used unless under strict regulations and after undergoing many stages of verification.” ³ This statement received backlash for intimidating foreign media. ⁴ In May 2020, the head of the SIS met with *Washington Post* and *New York Times* bureau chiefs to discuss “professional violations” in the outlets’ reports on Egypt. The SIS warned that “in the event that such professional violations... appropriate measures permitted by both the law in Egypt and the rules of many countries worldwide shall be taken against him.” ⁵

Inauthentic online behavior is an issue in Egypt. A report by Just Security identified examples of both progovernment and antigovernment online content manipulation in September 2020. According to the report, “thousands of tweets called for the downfall of President Abdel Fattah Sisi’s regime while others countered with pro-Sisi support. Both pro– and anti-regime hashtags bear well-known signs of coordinated inauthentic behavior, demonstrating that authoritarians and anti-authoritarians alike are manipulating the digital public sphere.” Despite this, it was confirmed that the Egyptian state is the “largest and most sophisticated” deployer of content manipulation. While small-scale demonstrations did occur in September 2020, Egyptian state media framed the antiregime social media trend as “a hashtag war against the Egyptian people.” ⁶

In their efforts to combat coordinated inauthentic behavior, Twitter and Facebook have reported multiple incidents of content and account removals in Egypt (see B2). In November 2020, Facebook removed 14 accounts, pages, and groups belonging to a network that targeted Egyptian and other audiences. Several Facebook and Instagram accounts associated with the Muslim Brotherhood were also removed. ⁷ In January 2021, Twitter disclosed “state-backed actors’ attempts to disrupt the conversation on the service” between January and June 2020. Twitter reported actions taken against 52,000 accounts ascribed to information operations in Egypt and several other countries. ⁸ In April 2020, Twitter reported the removal of 2,541 government-linked accounts. In September 2020, pro– and antigovernment Twitter hashtags were reportedly used in manipulation campaigns waged by pro– and antigovernment actors. ⁹

The authorities have created two WhatsApp groups to convey instructions to media outlets on what to report and what the redlines are. The group “Editors” is administered by the General Intelligence Service (GIS) and the second is administered by the Interior Ministry. In May 2019, media outlets were provided instructions through messages on the groups to abide by the ministry’s statement regarding the explosion near Cairo’s Grand Egyptian Museum, where at least 12 South African tourists were injured. In September 2019, media organizations were warned against reporting on former military contractor Mohamed Ali, who called for the September 2019 protests (see B8). ¹⁰ In January 2020, directions were

broadcasted to refrain from covering former US president Donald Trump's Middle East plan (dubbed the "peace plan" or "deal of the century") and to not touch upon its "violations of Egyptian and Arab principles regarding the Palestinian issue." The plan was barely criticized by any media outlet, short of a few independent online platforms. ¹¹

The Information Ministry has sought to improve its public opinion in the media by recruiting young Instagram influencers to their new media ambassadors' program. While it is unclear whether the government is paying the influencers, they have been told that the program will help boost their platforms and increase their followers. According to the *Guardian*, using social media influencers to try and reshape public opinion of the Egyptian government "projects a false narrative that undemocratic governments are listening to their citizens while masking a prolonged crackdown on free speech." ¹²

B6 0-3 pts

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

0 / 3

The economic viability of independent news sites is constantly under threat. Many of such outlets have closed, and others face financial troubles. Those subjected to blocking have suffered revenue losses, leading some to suspend their operations. ¹

In June 2019, the board of *Al-Tahrir*, whose website had been blocked since that May, announced that the newspaper would be bankrupt within two months if the website was not unblocked. The newspaper, though offered in print, secured 80 percent of its revenues via online advertisements. *Al-Tahrir* staff had sought all possible means to investigate the reasons behind the website's blocking. It contacted the SCMR, NTRA, MCIT, and ISPs, but no explanation was given. ²

In addition, the 2018 law on media regulation requires media outlets, defined to include any website or social media account with at least 5,000 subscribers, to pay a fee of 50,000 Egyptian pounds (\$3,200) to obtain a

license from the SCMR and gain legal status. ³ Outlets must also have at least 100,000 Egyptian pounds (\$6,400) in capital. The law allows sites to be blocked on several grounds, including spreading purportedly false news. ⁴ In October 2018, the SCMR started accepting applications for licenses even though the law's implementation guidelines had yet to be released. ⁵ In January 2019, the SCMR announced that 113 websites had applied for registration and the regulator extended the deadline to obtain a license until the end of the month. ⁶

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	2 / 4
--	--------------

At a time when traditional media have become increasingly consolidated in ownership and homogenized in content, online media have also struggled to maintain their independence and diversity of views given the arduous conditions of, and sweeping restrictions imposed by, new regulations and local practices. Egyptians resort to social media as the main source of information despite it also being monitored and censored (see B3 and C7).

According to the SimilarWeb ranking of the most widely visited websites in Egypt in 2018, Facebook and YouTube were the second and third most visited sites, respectively. ¹ In 2019, the most widely read news outlets, according to Alexa rankings, were primarily tabloids, news portals aligned with the government, and sports websites. ²

The blocking of hundreds of websites has negatively affected the diversity of media, and consequently of critical opinions. According to a 2018 survey conducted by Northwestern University in Qatar, only 3 percent of internet users in Egypt used VPNs, which can be employed to bypass blocking and reach obstructed sites. ³ Furthermore, 54 percent of 2019 respondents said that they feel comfortable speaking about politics, compared to 79 percent reported in 2018. Only 42 percent of respondents believed that Egyptians should be able to express ideas online even if they are unpopular. Some 60 percent believe that the internet should be

regulated, particularly to protect users' privacy and make the internet more affordable. ⁴

The RSF Media Ownership Monitor project highlighted several risks to media pluralism in Egypt, mostly to ownership concentration and transparency. ⁵ Nearly half of Egypt's popular media outlets are controlled by official agencies or intelligence services, while those that are not publicly owned are instead owned by progovernment businessmen. Independent outlets are either censored or blocked by authorities. ⁶

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	3 / 6
--	--------------

Digital activism and political organizing have been less prevalent in recent years due to widespread arrests, harsh prison sentences for dissidents and protesters, and the use of deadly force to suppress demonstrations.

¹ A law passed in 2013 effectively banned protests and gave police broad powers to crack down on unauthorized assemblies. ² At the end of the reporting period, numerous activists remained in jail for opposing the government.

Since April 2020, the authorities have cracked down on female TikTok users for allegedly "violating family values and principles" under Articles 25 and 26 of the cybercrime law (see B3). A number of women have been detained for similar morality-related charges and at least three received prison sentences (see C3). In solidarity with the convicted women on TikTok, an online female-led campaign circulated a petition on the hashtag "with permission from the Egyptian family." The campaign called for the women's release, condemned the arbitrary charges they received, and posited a petition entitled "if TikTok women are being punished for their content that 'violates... Egyptian family values,' could we at least know what those values are?" ³ In August 2020, Masaar disclosed that it filed a memorandum to the Cairo Misdemeanors Economic Court of Appeal in response to the TikTok crackdown, arguing that Article 25 of the

cybercrime law was unconstitutional. ⁴ Another related movement used the hashtag #MeToo to denounce male sexual violence. ⁵

In September 2019, social media users called for protests against President Sisi after businessman and former military contractor Mohamed Ali posted videos alleging corruption by the president. ⁶ In September 2019, thousands of citizens demonstrated in cities including Cairo and Alexandria. Security agents and police responded with force and arrested almost 2,000 people (see C3). ⁷ Ali called for another protest later that month, which did not happen because many dissenting voices and social media platforms were blocked online (see B1 and B8). ⁸ During the September demonstrations, police and plainclothes security forces seized and searched the mobile devices of citizens who were forced to unlock their devices and social media accounts, which were checked for evidence of antigovernment sentiment. ⁹ In the wake of the protests, disruptions to Facebook Messenger, Skype, and news sites were reported. ¹⁰ A number of other instant messaging applications were also blocked (see B1). ¹¹ The authorities arrested over 3,000 protesters, including 111 minors. Most of the arrested political activists, human rights advocates, and internet users were detained for being highly critical of the government online and offline. ¹²

Batel, which was launched to coordinate opposition to the April 2019 constitutional referendum that month, was blocked after 13 hours, having collected 60,000 signatures (see B1). ¹³

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
--	--------------

The constitution contains language that nominally guarantees freedom of the media, stating that Egyptians “have the right to own and issue

newspapers and establish visual, audio, and digital media outlets.” ¹ Under Article 34, the government is given the role of preserving online security, while under Article 70, “the law shall regulate ownership and establishment procedures for visual and radio broadcast stations in addition to online newspapers.” Article 71 forbids censorship “in any way,” and states that no individuals should be jailed for crimes committed through publication. However, exceptions are made for censorship in “times of war or general mobilization,” and penalties for “incitement to violence” and “discrimination amongst citizens, or impugning the honor of individuals” are to be specified by law. ² Article 211 outlines the establishment of a national media council tasked with regulating “the affairs of radio, television, and printed and digital press, among others” and ensuring that the press maintains a commitment to “professional and ethical standards, as well as national security needs.” The SCMR was created in 2016, with the power to fine and suspend media organizations. ³ The constitution permits the trial of civilians who break these laws in military courts, despite objections from political activists. ⁴

In April 2019, the parliament approved amendments to the constitution that would allow Sisi to stay in power until 2030, extending his current four-year term to six years and permitting him to seek an additional six-year term in 2024. Among other changes, the amendments granted the president greater control over the judiciary and expanded the political and judicial authority of the military. ⁵ The new provisions were confirmed in the deeply flawed referendum held later that month. ⁶

In November 2019, a Foreign Ministry spokesperson declared that freedom of expression is protected in Egypt, except when it targets state institutions, transcends the constitution or law, or violates international obligations. Finally, he asserted that only the judiciary can investigate these cases and that defendants have the rights and necessary safeguards to defend themselves. ⁷

C2 0-4 pts

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

0 / 4

The legal framework that governs online activity restricts freedom of expression in a variety of ways. Defamation is considered a criminal offense and included in the penal code. ¹

In June 2018, the parliament approved three laws regulating the media.

² The laws, which replaced existing legislation and were all signed by the president in August 2018, govern three official bodies: the National Press Authority, which mainly oversees state-owned print outlets; the National Media Authority, which is primarily responsible for state-owned broadcast outlets; and the SCMR, which supervises the media more broadly, including online media. The legislation regarding the SCMR, Law No. 180 of 2018, contained a number of new restrictions, stipulating that no media outlets could be established or managed in Egypt without an SCMR license. Moreover, the law defines media outlets to include blogs and personal social media accounts with at least 5,000 followers, subjecting the individuals behind them to account removal, fines, and imprisonment if they are found to be spreading purportedly false news (see B3 and B6). ³

In August 2018, the president signed the Anti-Cyber and Information Technology Crimes Law, or Law No. 175 of 2018. ⁴ It authorizes the blocking of websites that are deemed a threat to national security and punishes individuals who visit banned websites with up to one year in prison. Creators or managers of websites that are later banned could face up to two years in prison. ⁵

The 2015 antiterrorism law broadened the scope of crimes that are considered terrorism and prescribed harsh penalties for nonviolent acts.

⁶ Article 27 establishes a minimum five-year prison sentence for creating a website “with the goal of promoting ideas or beliefs” that incite violence, “broadcasting information to mislead the police or judicial authorities on terrorism cases,” or communicating with or organizing terrorist groups. ⁷ Setting up a group with the intention of “advocating by any means the obstruction of provisions of the constitution or laws” is punishable by life imprisonment or the death penalty. Activists argued that the broad language of the law could apply to any peaceful political party

or advocacy group. ⁸ Finally, journalists face heavy fines for disputing official accounts of militant attacks. In March 2019, a parliamentary committee proposed amendments that prescribe severe penalties for expressing opinions online. Ostensibly promoting extremist ideology could carry a 10-year prison sentence, while promoting terrorist acts, extremist ideology, or ideas and beliefs that advocate violence could result in imprisonment of 15 years. ⁹

In 2015, President Sisi issued a separate law broadening the definition of “terrorist entities” to include anyone who threatens public order “by any means,” allowing the state to draw up lists of alleged terrorists or terrorist organizations. ¹⁰ The law was met with skepticism from legal experts and human rights activists, who said that its vague wording could allow the state to designate political parties, student unions, or human rights organizations as terrorist groups. ¹¹ In February 2020, the parliament approved amendments to the definition of “a terrorist entity” and removed satellite channels, radio stations, and social media from the list of alleged terrorist groups in response to internal government backlash. Officials worried the broad definition of “terrorist entities” adversely impacted Egypt’s reputation regarding free speech. ¹²

Amendments to the law on states of emergency, the antiterrorism law, and the criminal code were rushed through in 2017 after terrorist attacks on three Coptic Christian churches. The amendments allowed for the indefinite detention of individuals suspected of threatening national security through the use of special emergency courts. The right to appeal the decisions of such courts and obtain a fair trial were curtailed. Police may also detain individuals for seven days without bringing them before a judge or prosecutor. ¹³ A similar law used during the era of former president Hosni Mubarak before 2011 was struck down by the Supreme Constitutional Court in 2013.

In May 2020, the month after an armed attack led to fatalities among security forces in North Sinai, ¹⁴ the parliament extended a state of emergency for three months. Also in May, President Sisi ratified amendments to the Emergency Law, No. 162 of 1958, granting more powers to the armed forces over civilians and providing further legal

grounds for military prosecution. ¹⁵ The state of emergency was still in effect at the end of the reporting period. The state of emergency was first introduced in April 2017 following a terrorist attack on three Coptic churches, and has since been renewed 11 times. Anyone who violates the state of emergency can be imprisoned. ¹⁶

In July 2020, the cabinet approved a criminal-code amendment that safeguards the privacy and anonymity of sexual-assault survivors and witnesses. The new amendment permits prosecutors to conceal identities and personal information of survivors in sexual-violence cases. ¹⁷

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?

0 / 6

Score Change: The score declined from 1 to 0 due to the continued practice of holding people in long pretrial detention for content posted online, as well as multiple long prison sentences handed out to social media users during the reporting period.

Internet users in Egypt operate in a highly repressive environment. According to the Committee to Protect Journalists (CPJ), Egypt remains one of the world's worst jailers of journalists. RSF's World Press Freedom Index 2020 ranks Egypt 166th out of 180 countries. ¹ Detainees have been subjected to mistreatment and torture in prison (see C7). In many cases, the government justifies these arrests under the guise of "counterterrorism." ² In addition to fines, arrests, and prison sentences, some civil society leaders faced travel bans and asset freezes during the reporting period. ³

In an effort to bypass the Criminal Procedures Law, which outlaws the extension of pretrial detention for more than four years, the authorities have embarked on a practice of "recycling defendants." ⁴ Many human rights activists received renewed detentions on old or new cases, including Mahienour El-Masry, Mohamed Ibrahim, Esraa Abdel Fattah, Solafa Magdy, Alaa Abdel Fattah, ⁵ Mohamed Gaber Soliman, ⁶

Hassan Mostafa, Hussein Khamis, ⁷ Mohamed Mamdouh Abdel Haleem, ⁸ Mohamed Saleh, ⁹ Ahmed Mohamed Hossny (also known as Ahmed Samy Shouib), Loay Mazhar, Adnan Alaa El-Deen, Saad Walid Saad, ¹⁰ and Ahmed Mohammad Abu Khalil. ¹¹

During its July-to-September 2020 reporting period, the AFTE documented examples of security forces targeting internet users for criticizing government policies; the organization counted 12 incidents during the period that included arrest, prosecution, and sentencing of social media users under existing legislation, including prison sentences against 8 social media users. ¹²

Demonstrators who opposed the decision to demolish unregistered homes and voiced other grievances against the government in September 2020 were met with arrests and force. ¹³ The Supreme State Security Prosecution (SSSP) charged defendants, including children, under cases 880/2020 (108 citizens) and 960/2020 (25 citizens), ¹⁴ and accused them of “joining a terrorist group, spreading false news, using social media accounts for the purpose of committing a crime, inciting assembly, and assaulting public officials.” ¹⁵

In March 2020, the public prosecutor vowed to issue fines or prison terms of as long as five years against those disseminating purportedly false COVID-19-related news. Authorities then embarked on a campaign of arrests where dozens of citizens, political activists, and individuals affiliated with state-owned or progovernment media institutions were detained over their social media content. ¹⁶ Most activists and social media users were targeted via cases N. 558/2020, the so-called “Corona Case,” and N. 535/2020. Detainees were accused of “belonging to a terrorist group and spreading fake news.” ¹⁷

The following were some of the more notable new criminal cases involving online posts and commentary during the coverage period:

- In June 2020, security forces raided the headquarters of the Al-Manassa website and arrested editor in chief Nora Younis, accusing her of “creating a website with the aim of committing a crime punishable by the law, possession of a software program developed

without the permission of the National Communications Regulatory Authority, infringement of literary and financial property rights, and unlawful use of information and telecommunication technology.” Al-Manassa was blocked and Younis was later released on 10,000 Egyptian pounds (\$630) bail. ¹⁸

- In June 2020, Sherifa Refaat and daughter Nora Hashem were detained and accused of “publishing scandalous videos that included sexual overtones.” They received prostitution convictions in September ¹⁹ and were handed six-year prison sentences and a fine of 100,000 Egyptian pounds (\$6,300). ²⁰
- In June 2020, belly dancer Sama El-Masry received a three-year sentence and a 300,000 Egyptian pound (\$18,900) fine for publishing videos on Facebook, Instagram, and YouTube that “violate public morality.” ²¹ In September, the court reduced the sentence to two years while sustaining the fine. ²²
- In June 2020, journalist Mohamed Monir was arrested by plainclothes security officers and was charged with “joining a terrorist group, spreading false news, and misusing social media.” According to surveillance videos published by Monir on his Facebook page and in news reports, Monir’s apartment was raided and searched by plainclothes security officers and then by armed security forces days before his arrest. Monir had previously written an article criticizing the government’s COVID-19 response for Al-Jazeera. ²³ In July, Monir was released after contracting COVID-19 in prison and died of complications soon after. ²⁴
- In July 2020, TikTok influencer Manar Samy was arrested after a lawsuit was filed against her for “posting short videos and pictures on Instagram and TikTok that contained sexual innuendo to provoke sexual arousal with the aim of attracting viewers, and collecting money in violation of the customs and traditions in the country.” Later that month, Samy was sentenced to three years in prison and a fine of 300,000 Egyptian pounds (\$18,500) for similar charges. ²⁵
- In August 2020, Mohamed al-Galali, the administrator of a “sexology” Facebook page, was arrested on debauchery-related charges, using a personal social media account to commit and facilitate the crime,

and violating family values and principles. He was later released on a bail of 2,000 Egyptian pounds (\$125). ²⁶

- In August 2020, prominent human rights defender Bahey eldin Hassan, director of the CIHRS, received a 15-year in absentia prison sentence, the longest sentence imposed on a human rights defender in Egypt. ²⁷ He was charged with “the use of social media to defame the judicial authority,” “the dissemination of false news with the aim of harming the country’s economic position,” and “disrupting the provisions of the constitution and law.” ²⁸ Hassan had criticized the Sisi regime on his Twitter account. ²⁹ He has been in self-exile in France since 2014. ³⁰
- In September 2020, Kamal El-Balshy, the brother of human rights defender Khaled El-Balshy, founder and editor in chief of the blocked Darb news site, was detained. He later received charges of illegal assembly, membership of a banned group, spreading false news, and misusing social media. ³¹
- In September 2020, journalist Islam al-Kalhi was arrested while covering the al-Moneeb protests. The SSSP added him to case 855/2020, held him in pretrial detention, and charged him with “belonging to a terrorist group, publishing false news and misusing social media.” ³²
- In November 2020, Egyptian Initiative for Personal Rights executive director Gasser Abdel Razek, criminal-justice unit director Karim Ennarah, and administrative manager Mohamed Basheer were arrested and held in pretrial detention. The SSSP charged them with joining a terrorist group, spreading false news, and misusing social media. They remained in pretrial detention for 15 days. Abdel Razek reported mistreatment in detention, where he was not allowed to leave his cell. ³³ In February 2021, the three were released on bail. ³⁴
- In November 2020, video blogger Shadi Abu Zeid was given a six-month prison sentence for insulting a government official in a Facebook post. Such charges are reportedly linked to a video published by Abu Zeid's satirical news and interview program, *The Rich Content*. ³⁵

- In December 2020, columnist Aamer Abdelmonem was arrested and charged with “spreading false news and assisting a terrorist organization,” and held in pretrial detention for 15 days. Shortly before his arrest, he published an article criticizing the government’s COVID-19 response in Al-Jazeera. Abdelmonem, who is diabetic and has cataracts in both eyes, was denied medication while in detention. ³⁶
- In January 2021, cartoonist Ashraf Hamdy Hamdy was arrested at his home after posting a cartoon video applauding the youth of the revolution on his YouTube channel, Egyptoon. He was charged with misusing social media and spreading false news. ³⁷
- In March 2021, human rights activist Sanaa Seif was sentenced to 18 months in prison for “broadcasting fake news and rumors” regarding the spread of COVID-19 and health conditions in Egypt. ³⁸ The ruling refers to other charges including a six-month prison sentence for insulting a public employee while performing his job, in reference to her visit to brother Alaa Abdel Fattah in the Tora prison (see C7). ³⁹
- In April 2020, university student Haneen Hossam was detained for allegedly “inciting debauchery” and “promoting human trafficking” among Egyptian women on TikTok by publishing a video explaining how to use the app for financial gain. ⁴⁰ That July, the Cairo Economic Misdemeanor Court sentenced her to two years in prison and a fine of 300,000 Egyptian pounds (\$19,000). ⁴¹
- In May 2020, social media influencer and director of the Likee app, Mawada Eladhm, was detained for “violating family principles and values in Egyptian society” and “establishing, managing, and using [websites and social media accounts] with the aim of committing those crimes.” In July, Eladhm, Likee staff member Mohamed Abdel Hamid Zaki, Mohamed Alaa El-Din Ahmed, and Ahmed Sameh Attia were each sentenced to two years in prison and 300,000 Egyptian pound (\$18,540) fines. Eladhm was charged with posting “indecent” dance videos and “violating the values and principles of the Egyptian family,” inciting “debauchery,” evading justice, and encrypting their phones and personal accounts. ⁴²

The following are examples from the coverage period of the Egyptian authorities' practice of recycling detainees. These people were charged before the coverage period, then received new sentences during this coverage period:

- In September 2019, blogger Mohamed Ibrahim (also known as Mohamed Oxygen) was arrested on new charges after being released on probation in July 2019. Ibrahim was detained while visiting a police station as part of his probation conditions. In October 2019, a Cairo criminal court ordered him detained on charges related to “membership of a terrorist organization,” “defamation,” and “misuse of social media.” ⁴³ On February 1, 2020, his detention was renewed for 15 days. ⁴⁴ Shortly before his expected November 2020 release date, he received an additional charge for membership of a terrorist organization and was detained pending an investigation. ⁴⁵ He was awaiting sentencing at the end of the coverage period.
- In September 2019, prominent activist and lawyer Mahienour El-Masry was arrested in front of the SSSP building and was added to case 488/2019 despite not being part of the September 2019 protests. El-Masry was then held in pretrial detention. ⁴⁶ ⁴⁷ Her detention was renewed for 45 days in December 2020 and again in January 2021. ⁴⁸ She was still detained at the end of the coverage period.
- In September 2019, photographer Sayed Abd Ellah, who was livestreaming the antigovernment protest in Suez, was arrested. The police physically attacked his wife and children and insulted him for his social media posts. He was charged with “membership in a banned group,” “spreading false news,” and “misusing social media platforms to disrupt national security.” ⁴⁹ In November 2020, the court ordered the release of Abd Ellah. ⁵⁰ Later that month, he was arrested again, issued new charges of membership in a terrorist group, and held in pretrial detention. ⁵¹ He was still detained at the end of the coverage period.
- In September 2019, Alaa Abdel Fattah, a prominent activist and blogger, who was jailed for five years and released on probation in March 2019, was arrested and taken into SSSP custody. It was

reported that Abdel Fattah was beaten and insulted during his detention in Tora. ⁵² In July 2020, Abdel Fattah's detention was renewed for the third time, pending investigations in case 1356/2019.

⁵³ As of the end of the reporting period, he was still awaiting trial. ⁵⁴

- In October 2019, reporter, blogger, and Tahrir News social media coordinator Esraa Abdel Fattah, was arrested by plainclothes security officers and was reportedly beaten and forced to surrender her mobile-phone password. ⁵⁵ In June 2020, Abdel Fattah's court session, meant to determine the renewal of her detention, was postponed. ⁵⁶ Her detention was further renewed several times pending an ongoing investigation. ⁵⁷ She was still detained at the end of the coverage period. ⁵⁸
- In November 2019, freelance reporter Solafa Magdy, blogger and freelance journalist Mohamed Salah, and freelance photojournalist Hossam El-Sayyad were arrested by plainclothes security officers and taken to a police station after leaving a coffee shop. Their mobile phones were reportedly confiscated and Magdy was beaten. Later that month, a state security prosecutor charged all three with membership in a banned group, and Magdy and Salah of disseminating false news. ⁵⁹ In August 2020, the state prosecutor's office issued the three defendants new charges for actions they allegedly committed while in prison, accused them of membership in a terrorist group and of spreading false news, and extended their pretrial detention. ⁶⁰ In April 2021, Magdy and El-Sayyad were released. ⁶¹
- In March 2020, after publishing a Facebook post questioning official COVID-19 statistics, Alkarar Press editor in chief Atef Hasballah was arrested. He disappeared for almost a month but the SSSP ordered his pretrial detention on several charges including "joining a terrorist organization" and "spreading false news" that April. ⁶² In December 2020, Hasballah's detention was renewed for 45 days. ⁶³ He was released in March 2021. ⁶⁴

Multiple prominent digital activists and online journalists remain in prison. In many cases, the individuals faced charges unrelated to their online activities, although their supporters argue that they were arrested to

prevent them from expressing their views. Spreading false news, affiliation with a terrorist group, insulting the state, and inciting demonstrations are the prevailing allegations used to justify the arrest of human rights activists.

The campaign of Egyptian authorities to crack down on dissenting voices undermines international human rights law and internet freedoms. These moves have been criticized by local and international human rights organizations alongside intergovernmental organizations.

According to a 2019 Amnesty International report, the SSSP is “misusing counter-terror legislation to prosecute thousands of peaceful critics and suspend guarantees to fair trial.” The report sheds light on some SSSP practices, including arbitrary detention, denial of effective legal representation, coercive questioning, prolonged pretrial detention, the denial of the right to challenge charges, torture, and enforced disappearances. ⁶⁵ In September 2020, the International Commission of Jurists and the Tahrir Institute for Middle East Policy released a report focusing on the crackdown against lawyers by authorities, particularly the SSSP. Lawyers have been charged with “terrorism,” “spreading false news,” and “misusing social media.” According to the report, these charges have intimidated lawyers and encouraged them to halt their work and avoid challenging prosecutors or supporting detainees during interrogations. ⁶⁶

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?

1 / 4

The NTRA’s 2010 regulation of the registration of consumers’ personal data in selling and activating mobile lines requires distributors of SIM cards to collect the personal data from buyers’ identification documents before the cards can be activated. ¹ This threatens the anonymity of communication as well as the privacy and protection of personal data. In recent years, the NTRA has sought to remove dormant and unregistered SIMs to promote the credibility of the Egyptian market. ²

Individuals seeking to register a web address using Egypt's .eg domain must submit their personal data and copies of their national identification document.

Encryption remains restricted. Article 64 of the Telecommunication Regulation Law outlaws the use by telecommunications companies, their employees, or their customers of any encryption equipment without written consent from the NTRA and security agencies. ³ In a November 2018 report, freedom-of-expression group Article 19 criticized Article 72 of Law No. 180 for granting the SCMR exclusive control over the establishment of encrypted platforms and requiring government approval for any other usage of such platforms. ⁴

C5 0-6 pts

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

1 / 6

Surveillance is a significant concern for internet users in Egypt. Article 57 of the constitution states that private communications “may only be confiscated, examined, or monitored by causal judicial order, for a limited period of time, and in cases specified by the law.” Judicial warrants are needed for authorities to enter, search, or monitor private property such as homes, as specified in Article 58. In practice, surveillance operations lack transparency, potentially violating the constitution's privacy protections. Additionally, Article 95 of the criminal code provides legal authority to law enforcement agencies to request the disclosure of communications data. ¹

The cybercrime law (see C2) provides national security agencies access to the electronic data of internet and communication platform users without judicial oversight or clear regulation. Additionally, it does not include any substantial means to mitigate privacy violations or any compensation for the ensued harm from these violations. ²

In October 2020, it was reported that the Egyptian government was using Sandvine devices to block websites (see B1). Additionally, Sandvine

technology employs DPI, which has troubling surveillance implications. The devices, which are used in the infrastructure of some service providers, allow operators to obtain information about users' behavior, prevent or tamper with connections, and monitor connections, especially if users themselves are not employing encrypted technology. ³

In September 2020, Amnesty International's Security Lab reported new examples of FinSpy being used against Windows and Android devices, along with previously unknown versions targeting Linux and macOS computers. While Amnesty International previously reported on phishing attacks launched by the NilePhish attacker group, it did not directly link NilePhish to the use of FinFisher products. ⁴

Research and leaked documents have shown that Egyptian authorities have purchased or received surveillance equipment from international companies like Blue Coat, ⁵ Nokia Siemens Network, ⁶ Hacking Team, ⁷ Gamma Group, Ercom, and Amesys. ⁸ Following pressure from human rights organizations, the Italian government revoked authorization for surveillance company Area SpA to sell equipment to the Egyptian Technical Research Department in early 2016. ⁹

A provision of the antiterrorism law allows the police to monitor internet traffic and social media activity to "prevent their use for terrorist purposes."

¹⁰ A committee established by the NTRA tracks communications over VoIP services (see A3). The 2018 cybercrime law also facilitates surveillance by state authorities (see C6). Amid allegations that the government was monitoring communications over Facebook and Twitter, the MCIT asserted in March 2019 that the law does not provide for social media monitoring. Instead, the ministry said, it focuses on protecting privacy and personal data. ¹¹ Sheikh Shawki Allam, the country's grand mufti, has encouraged the screening of social media sites, claiming that a number of them promote false news. ¹²

In a 2018 report by Citizen Lab, a Canadian internet watchdog, Egypt is listed as one of 45 countries worldwide in which devices were likely breached by Pegasus, a targeted spyware software developed by the NSO Group, an Israeli technology firm. Pegasus is known to be used by

governments to spy on journalists, human rights defenders, and the opposition, though it is unclear whether the Egyptian government is a Pegasus client. ¹³

A December 2018 European Parliament resolution noted that Egypt has bought surveillance equipment from European companies that enables hacking and the exploitation of malicious software. This technology has contributed to the crackdown against freedom of expression online. ¹⁴ In July 2018, the International Federation for Human Rights reported that technical assistance from the French government and private sector has helped Egyptian authorities control internet infrastructure, monitor communications, and crack down on dissent. ¹⁵

In October 2019, cybersecurity company Check Point reported that Egyptian citizens were targeted through sophisticated spyware in downloaded apps, enabling attackers to read emails, log contacts, and record locations of citizens. The central server used in the attacks was linked to the Egyptian government (see C8). ¹⁶

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	0 / 6
---	--------------

The government can obtain user information from companies without due process. Article 64 of the Telecommunication Regulation Law allows service providers, as well as their marketing agents, to collect “accurate information and data” from “individuals and various entities within the state.” It also compels providers to give security agencies access to their “equipment, systems, software, and communication.” ¹

According to Privacy International, the 2018 cybercrime law “forces telecommunications providers, specifically ISPs, to provide technical assistance” to law enforcement and their surveillance operations. The law also compels providers “to collect data, including personal identifiers, metadata, and ‘other data’ not specified by the law and store them for a default period of 180 days.” ² Failure to retain data for this amount of

time could result in a fine of up to 10 million Egyptian pounds (\$637,000); a second violation can lead to a fine of 20 million pounds (\$1.3 million) and revocation of the company's license. ³ State agencies can request stored data without a judicial order, ⁴ an apparent violation of Article 57 of the constitution (see C5). ⁵

A draft data-protection law endorsed by a parliamentary committee in November 2019 would protect certain types of user data and establish a center to monitor compliance with the law. ⁶ However, the same bill stipulated that service providers should retain users' data for 180 days and provide access to state authorities upon request. ⁷ The legislation, which was approved by the parliament in June 2019 and ratified by the president in July 2020, is the first legal safeguard to address individual data privacy, and contains some data-protection principles. ⁸ However, the law exempts national security authorities from user-data protection obligations. It also does not include guarantees to the independence of the Personal Data Protection Center, which will be the regulatory authority. ⁹ In March 2021, there was a stakeholder discussion on the application of the law. ¹⁰

The ICT minister described plans in March 2018 to create an Egyptian version of Facebook. A locally based social media company would presumably be easier for the government to coerce into providing data on its users (see B3).

In 2017, the Egyptian government requested access to the internal software of ride-sharing apps like Uber and Careem, including data about customers, drivers, and journeys. Uber rejected the request, but in a meeting with Egyptian military intelligence, Careem executives were reportedly offered preferential treatment if they agreed to provide the data. The company said no such deal was implemented. ¹¹

In March 2018, Uber and Careem were banned by Cairo's administrative court after 42 taxi drivers filed a lawsuit against them. However, in April 2018, another court suspended the ruling until the higher administrative court could deliver a final verdict. ¹² In May 2018, the parliament passed a law to regulate ride-sharing apps, ¹³ requiring that the companies

obtain a five-year renewable license for a fee of 30 million Egyptian pounds (\$1.9 million), that drivers pay annual fees to obtain special licenses, and that the companies retain user data for 180 days and share it with authorities “on request” and “according to the law.” ¹⁴ Requests for data do not need to be accompanied by a warrant, though a decree from the prime minister is required. ¹⁵ Following the law’s ratification in June 2018, negotiations between Uber and the government on implementing regulations were reportedly suspended in January 2019 due to controversy over whether the legislation can require user data to be stored in Egypt and whether security agencies can access it. ¹⁶ According to legal analysts, however, a data localization requirement is not enshrined in the law. ¹⁷

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?	1 / 5
--	--------------

Imprisoned activists, bloggers, and journalists frequently experience abuse and torture while in detention. They are subject to lengthy pretrial detention, which in some cases lasts for years (see C3).

Since the beginning of the COVID-19 pandemic, Egyptian authorities banned visits to detainees to contain the spread of the pandemic, but have refrained from disclosing coronavirus-mitigation plans within the prison system. In August 2020, family visits were allowed but with some restrictions. ¹ Additionally, prisoners of conscience were denied medical treatment through deliberate denial or negligence. ² Furthermore, torture in prisons is not uncommon. Galal El-Behairy, the poet imprisoned in June 2018 after writing an antigovernment song that spread online, was reportedly tortured in detention. ³

According to HRW, the LGBT+ community has been targeted by security forces on social networking sites and dating apps. ⁴ In March 2019, a transgender woman, Malik al-Kashef, was arrested and accused of involvement with a terrorist group and using social media to disrupt public

order. She reportedly suffered sexual harassment and a forced anal examination in custody (see C3). ⁵ In July 2020, “Rami” (whose legal name was withheld for safety reasons) was harassed on Facebook for being perceived as gay and was later harassed and assaulted offline. Rami had posted a TikTok video in front of a rainbow flag, which was uploaded on Facebook without his permission. He started receiving intimidating messages and a death threat, prompting him to temporarily close his account (see B4). ⁶

Bloggers are frequently intimidated online by government supporters, who often work in collaboration with progovernment news sites to smear prominent opponents. For example, Esraa Abdel Fattah, who was arrested in October 2019 and accused as part of case 488/2019 (see C3), was attacked by progovernment media outlets that condemned her for being dishonest about her torture during interrogation. Abdel Fattah was dubbed an “agent of chaos for the Muslim Brotherhood.” ⁷

In February 2020, Patrick George Zaki was detained and held for 24 hours by Egyptian authorities and was subjected to torture, including with electric shocks, according to HRW. Zaki, a researcher and activist, was accused of “calling for protests without permission” and for “spreading false news and inciting violence and terrorism” after posting to his Facebook page. ⁸ His Facebook posts were the focal point of his interrogation, according to HRW.

Following the September 2019 protests, police and plainclothes security agents searched and seized mobile devices. People were asked to unlock their mobile phones and provide access to their social media accounts, which were checked for any expression of antigovernment sentiment (see C5). It was reported that these actions were legal as the public prosecutor had issued an order to inspect the social media accounts of allegedly illegal protesters. ⁹ These practices continued even after protests subsided. There were reports of citizens being stopped and their phones being searched at police checkpoints. In the first quarter of 2020, an individual, whose name was withheld by his family, disappeared after the police found antigovernment social media posts when accessing his mobile phone at a checkpoint. He was later charged via case 65/2021 for

joining a terrorist group and spreading false news on social media (see C3). ¹⁰

In November 2019, after *Mada Masr* published an article on Sisi's eldest son, who had been sidelined from his government position, nine plainclothes security officers raided the outlet's office. They confiscated laptops and phones and took three staff members for interrogation who were later released. ¹¹ A Foreign Ministry spokesperson highlighted that all procedures taken in the *Mada Masr* raid were legal and that *Mada Masr* did not have the required license to operate. He further denied any detentions of staff and claimed that security agents did nothing beyond inspection, interrogation, and investigation. ¹²

In January 2020, police raided the Turkish state-run Anadolu News Agency office in Cairo and arrested four people, including a Turkish administrator and two Egyptian journalists, for allegedly spreading false news and operating without a license. The police examined phones, computers, and documents and then took the detainees to an unknown location. ¹³

The Egyptian authorities frequently arrest, torture, and mistreat journalists and their families in an effort to silence them and retaliate against their reporting on human rights violations. In June 2020, activist Alaa Abdel Fattah's mother, Leila Soueif, and sisters Sanaa Seif and Mona Seif, were not allowed to visit Abdel Fattah in prison, deliver food, or deliver a letter. When they refused to leave, they were reportedly harassed and threatened. ¹⁴ In June 2020, Mona Seif was arrested in the Public Prosecutor's office when she went to file a complaint for the assault that her family was subjected to while visiting her brother in prison (see C3).

In July 2020, an Instagram account which published testimonies about a disinformation campaign targeting a rape survivor and witnesses in a rape case known as "the Fairmont incident" was subjected to online harassment and intimidation. Private information of arrested witnesses was leaked to social media and progovernment websites in a reportedly state-sanctioned disinformation campaign meant to defame the witnesses and portray the incident as "a group sex party" (see B5). ¹⁵ The

anonymous Instagram account that included testimonies on the incident were hacked (see C8). ¹⁶

During the coverage period, female social media influencers were subject to sexual assault, privacy violations, and online abuse. Women were investigated by the Morality Directorate of the Interior Ministry due to “the way they dress, act, ‘influence’ the broader public on social media, and earn money online.” A number of lawsuits were filed by men who objected to their online conduct. ¹⁷ Additionally, the authorities launched a targeted campaign against female TikTok users, with multiple women detained over accusations of prostitution, human trafficking, and “profiting off the internet” (see C3). Most of the women were accused of seeking illicit means to earn money and recruiting others to do the same. Amnesty International condemned the government’s “new repressive tactics to control cyber space by policing women’s bodies and conduct and by undermining their ability to earn an independent living.” ¹⁸

In July 2020, a disinformation campaign was waged against the survivor and witnesses of the Fairmont incident, where at least seven wealthy and well-connected men reportedly drugged and raped an 18-year-old woman in a hotel room at Cairo’s Fairmont Nile City Hotel in 2014 and subsequently shared video footage of the rape (see B5). After testimonies were published on an anonymous Instagram account, the account was exposed to hacking attempts (see C8), online harassment, and intimidation. Shortly after the arrests of the witnesses and campaigners, their private information was further leaked to social media in a reportedly state-sanctioned disinformation campaign aiming at defaming the witnesses and dubbing the incident “a group sex party.” ¹⁹

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
--	--------------

Internet users in Egypt have been subject to several internal and external cyberattacks in recent years.

The country was struck by several cyberattacks that used ransomware and affected companies worldwide in 2017. ¹ In addition, a 2018 Citizen Lab report found that Telecom Egypt had been redirecting Egyptian internet users to malware that mines cryptocurrency or displays advertisements, apparently to generate revenue using Sandvine equipment. ²

In March 2019, the International Telecommunication Union ranked Egypt 23rd out of 165 countries in its 2018 Global Cybersecurity Index, which could indicate its commitment to cybersecurity. ³ However, cybersecurity company Trend Micro released a March 2018 report finding that Egypt was the third most vulnerable country in Africa to malware attacks, after South Africa and Morocco. The manufacturing, education, government, real estate, and technology sectors were the most targeted. ⁴

In July 2018, US cybersecurity firm Symantec reported on a new espionage campaign named “Leafminer,” allegedly led by a group based in Iran that had targeted the Middle East region—including Egypt—to gain access to the emails, files, and databases of governments and businesses since early 2017. The group penetrated networks by infecting websites that the entities might use with malware, scanning networks for vulnerabilities, and systematically attempting to log in to user accounts. ⁵

In March 2019, Amnesty International reported “OAuth” phishing attacks using third-party applications against journalists and human rights activists that were most probably conducted by or on behalf of the Egyptian authorities and linked to the NilePhish attacker group. ⁶

In October 2019, Check Point published a report revealing Egyptian citizens were targeted through sophisticated spyware that allowed attackers to read emails, log contacts, and record locations through downloaded mobile-phone apps. Some of the apps identified in the reports include Secure Mail, iCloud200%, and IndexY. Check Point suggested that such operations were linked to the Egyptian government given the groups that were targeted, the government’s investment of human and financial resources, the structures and data downloaded, the use of a registered server belonging to the MCIT, and geographic

coordinates corresponding to GIS headquarters. The report identified 33 individuals—including journalists, politicians, activists, and lawyers—who were specifically targeted. ⁷

In July 2020, an Instagram account containing statements regarding the Fairmont incident was hacked by an unknown party (see C7). ⁸



On Egypt

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

[See More >](#)

Country Facts

Global Freedom Score

18/100 Not Free

Internet Freedom Score

26/100 Not Free

Freedom in the World Status

Not Free

Networks Restricted

No

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

[Freedom in the World 2021](#)

Other Years

2020

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

Email

Join the Freedom
House monthly
newsletter

Subscribe

ADDRESS

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

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org

@2022 FreedomHouse