Freedom House

FREEDOM ON THE NET 2024

Egypt

NOT FREE

28

/100

A. Obstacles to Access	**14**	/25
B. Limits on Content	**9**	/35
C. Violations of User Rights	**5**	/40

LAST YEAR'S SCORE & STATUS

28 /100   **Not Free**

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

Key Developments, June 1, 2023 - May 31, 2024

Internet freedom and the rights of internet users remained severely constrained in Egypt during the coverage period. Criminal penalties, harassment, and surveillance have contributed to high levels of self-censorship among Egyptian internet users. Activists, bloggers, and journalists who are arrested routinely suffer abuse and torture in detention.

- In October 2023, the Supreme Council for Media Regulation (SCMR) announced a six-month blocking of Mada Masr, an independent website known for its criticism of the government. Mada Masr's editor in chief Lina Attalah also faced criminal charges for her work (see B1 and C3).
- At least two other independent news websites were blocked for failure to obtain licenses, and in June 2024, after the coverage period, the SCMR and the National Telecommunications Regulatory Authority (NTRA) announced plans to block all unlicensed platforms (see B1 and B6).
- Ahead of Egypt's December 2023 presidential elections, the phone of Ahmed Tantawi, the most prominent potential challenger for President Sisi, was infected with Predator spyware, likely at the behest of the Egyptian security services (see B8 and C5).
- In July 2023, Patrick George Zaki, a researcher and activist, received a presidential pardon just days after being sentenced to three years in prison on charges of "spreading false news" after he published an online article about discrimination faced by Coptic Christians in Egypt (see C3).

Political overview

President Abdel Fattah al-Sisi, who first took power in a 2013 coup, governs Egypt in an 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 remains a serious problem, as do high rates of gender-based violence.

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

The Egyptian government has made efforts to improve the country's 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. As of January 2024, there were 82.01 million internet users in Egypt, representing an internet penetration rate of 72.2 percent.   **1**   Mobile usage is more widespread, with approximately 97.3 percent of the population accessing the internet via mobile connections.   **2**   According to Egypt's Ministry of Communication and Information Technology (MCIT), the share of Egyptian mobile users has increased steadily over the past two years.   **3**   According to the 2023 Network Readiness Index, Egypt ranked 46th out of 134 countries on their indicator examining the scale of the population covered by at least a third-generation (3G) mobile network.   **4**

Despite increases in access, internet speeds remain unreliable in Egypt. As of June 2024, Egypt ranked 107th globally in terms of mobile internet speed, with median download speeds of 24.39 megabits per second (Mbps) and median upload speeds of 5.76 Mbps. For broadband speeds, Egypt ranked 79th globally, with median download speeds of 75.44 Mbps and median upload speeds of 16.24 Mbps.   **5**   According to the 2023 Network Readiness Index, Egypt ranked 18th out of 134 countries on their international internet bandwidth indicator.   **6**

Since July 2023, power outages resulting from the government's "load-shedding" initiative has limited people's ability to access fixed-line internet. Under the initiative, to reduce electricity consumption during the summer months, the government imposed daily power cuts lasting one to two hours. Although officials pledged that the electricity crisis would be resolved by October 2023, the outages continued with similar intensity throughout the coverage period.   **7**   These power

outages have disrupted internet connectivity for both fixed-line and mobile connections, as fourth-generation (4G) tower providers across Egypt have also been affected.

The ICT sector in Egypt has demonstrated significant growth in recent years, due in part to increased government investment in ICT infrastructure, and the National Telecommunication Regulatory Authority (NTRA) has enacted reforms to upgrade the telecommunications infrastructure and increase internet speeds. [8] In January 2024, a $150 million contract was signed between the NTRA and Telecom Egypt for the provision of fifth-generation (5G) services across Egypt. [9]

Previous endeavors by the NTRA include the deployment of updated mobile technology in cooperation with telecom companies across the country since 2018. [10] In November 2021, the NTRA approved new frequencies for mobile operators with the goal of enhancing the quality of voice and data services. [11] In January 2022, the MCIT began an initiative to improve internet access in remote villages, with 33 villages participating in the project. As of December 2021, six villages had new fixed-line cables installed, and seven 4G base stations had been made fully operational. [12]

In September 2021, Telecom Egypt announced that it would improve the country's ICT infrastructure and secure access to high-speed internet services by providing fiber-optic networks to approximately 1,413 rural villages and towns. [13] This included providing internet services to 2,563 high schools and connecting 18,000 governmental buildings to fiber-optic cables. [14]

In February 2022, Egypt and Greece signed an agreement to extend a submarine fiber-optic cable between the two countries at a cost of $60 million. [15] In March 2022, Telecom Egypt announced the creation of a new route for fiber-optic internet cables between the Red Sea and the Mediterranean via Al Morshedeen Road, aiming to promote Egypt as a central point for intercontinental communications. [16] In 2023, Telecom Egypt entered into a joint project to link Egyptian and African networks via the European Medusa Submarine Cable System and the 2Africa subsea internet cable. [17] Once completed, the 2Africa cable will be the world's longest submarine communications cable and will provide connections to 33 countries.

In late November 2023, Telecom Egypt partnered with the Internet Corporation for Assigned Names and Numbers (ICANN) to install a Managed Root Server (IMRS) in Egypt. The IMRS would serve as a local response center for all domain name system (DNS) queries from Africa, which will reduce service providers' reliance on regional servers, improve internet speeds, and reduce vulnerabilities to cyberattacks (see C8). [18]

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?	**2**/3

Internet and mobile service prices are relatively affordable in Egypt; however, high inflation and price increases negatively impacted affordability during the coverage period. Egypt has undergone three currency depreciations in recent years and inflation surged to 34.6 percent in November 2023. [19] Based on 2022 data from the World Bank, the most recent data available, Egypt's gross domestic product (GDP) per capita is estimated to be 203,569.31 Egyptian pounds ($6,580). [20]

In addition to rising inflation, telecommunications operators have also increased prices. In February 2024, Egyptian telecom operators increased prices between 10 and 16 percent for mobile phone services, including both cellular and data charges. [21] Moreover, state-controlled operator Telecom Egypt raised the prices of its broadband internet services by around 33 percent, with private providers like Vodafone and Orange adjusting their broadband prices accordingly. This marked the first adjustment to mobile and internet service prices in Egypt since 2017. [22] A monthly mobile data package from Telecom Egypt can cost up to 450 Egyptian pounds ($14.50) or around 2 percent of an average monthly salary in Egypt. [23]

According to a 2023 report from Cable, a London-based price comparison website for broadband and mobile internet prices globally, Egypt was ranked 5th out of 219 countries for consumer broadband prices, with an average monthly package price of $8.31. For mobile data pricing, Egypt ranked 62nd out of 230 countries, with an average price of $0.65 per 1 gigabyte (GB) as of July 2023. [24]

There are regional disparities in internet access and infrastructure including the distribution of Asymmetric Digital Subscriber Line (ADSL) subscriptions across Egypt. In January 2024, ADSL subscriptions were concentrated in urban centers and densely populated regions, such as greater Cairo and the Nile Delta region, each of which claims 35 percent of the country's total ADSL subscriptions. In contrast, the more rural areas of Upper Egypt represent only 15 percent of ADSL subscriptions. Alexandria and Matrouh together account for 9 percent of subscriptions, while the Sinai, Red Sea, and Suez Canal areas collectively comprise only 6 percent of subscriptions. [25]

Alongside the geographical digital divide, a gender-based digital gap is also observed. Despite the overall increase in internet usage, Arab nations confront the most significant gender disparity in digital access globally. According to a 2021 report from the Wilson Center, 63 million women in the Middle East and North Africa region lack access to mobile internet, which serves as a critical gateway to online content for most individuals. [26] According to the World Economic Forum's 2020 Global Gender Gap Report, in Egypt, women fall behind men in terms of access to information technology and communications skills and services. [27]

A3 0-6 pts

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

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

Article 67 of the 2003 Telecommunication Regulation Law provides Egyptian authorities with the power to commandeer telecommunication services and networks of any operator or service provider. 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 in the event of cases listed under Article 67, such as "natural or environmental disasters" or "any other cases concerning national security." [28]

The government has centralized the internet infrastructure and fiber-optic cables to create highly controllable choke points. [29] In addition, virtually all of Egypt's

telecommunications infrastructure belongs to Telecom Egypt. Decree 242, issued in 2019, put the telecommunications infrastructure under the ownership of the National Service Projects Organization (NSPO), which is run by the Egyptian ministry of defense. **30**

Voice over Internet Protocol (VoIP) services have been intermittently blocked on mobile networks. 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. **31** The NTRA provided no justification for these disruptions. During the 27th UN Climate Change Conference (COP27) in November 2022, Egyptian telecom providers lifted the ban on WhatsApp VoIP services, such as voice calls, for a short period of time (see B1). **32** However, the restrictions were restored after the conference.

Periodic blockages of VoIP traffic over mobile networks were documented as early as 2010, **33** and in 2013, the NTRA announced the establishment of a committee to "monitor" communications on WhatsApp and Viber. **34** Making international calls over VoIP networks is technically illegal under Article 72 of the Telecommunication Regulation Law. **35**

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, at 40.5 percent, while Orange Egypt, a French company, has 33 percent. **36** Etisalat Misr, with its 24 percent market share, is 66 percent owned by Etisalat, which has strong ties to the United Arab Emirates (UAE). **37** In 2017, state-owned Telecom Egypt officially launched We, **38** the country's fourth mobile network. Telecom Egypt also owns about 45 percent of Vodafone Egypt.

Telecom Egypt, under the banner WE, controls 80.1 percent of the ADSL market. Egypt's other main internet service providers (ISPs) are Etisalat Egypt, Noor, and Vodafone Data. **39** These companies lease lines from WE and resell bandwidth to

smaller ISPs. **40** In 2016, Etisalat Misr obtained a license to offer fixed-line services via Telecom Egypt's infrastructure. **41**

In 2022, Vodafone International Group approved the transfer of 55 percent of its shares in Vodafone Egypt to Vodacom (its sub-Saharan African subsidiary) in exchange for cash and new shares in Vodacom. **42** Vodacom announced that it will "sign [a] deed of adherence to the shareholders' agreement with Telecom Egypt," **43** which owns 44.95 percent of Vodafone Egypt. **44**

The NTRA and the MCIT issue guidelines for ISPs and regulate licensing. These guidelines at times undermine a competitive telecommunications market. Unlike international best practices, the guidelines for granting licenses to ISPs do not refer to any standardized economic model for determining service prices. There is no reference to common pricing methods, such as usage-based pricing, flat-rate pricing, or pricing supported by both the user and the service provider, giving ISPs significant leeway to set their prices in ways that could harm consumers. **45**

In late December 2022, amendments to the 2003 Telecommunication Regulation Law broadened the scope of prohibited activities for ISPs. Under the amended law, companies must obtain a permit from the NTRA and other relevant bodies to use, operate, install, or sell any ITC equipment. Violation of the law could result in a fine between 2 and 5 million Egyptian pounds (between $64,630 and $161,590). **46**

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 Telecommunication Regulation Law, which does not guarantee the NTRA's independence. **47**

The authority is subordinated to the MCIT, and the members of its board are selected by the prime minister, who also determines their salaries. **48** The NTRA board is chaired by the minister of communications and information technology and includes representatives from the ministries of defense, finance, and interior; the National Security Council; the presidency; and trade unions, among others. **49**

Officially, the NTRA is responsible for ensuring a competitive market environment, managing the frequency spectrum, setting industry standards, and overseeing interconnection agreements. **50**

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 to be an infringement on the right to communicate, among others. **51**

In December 2023, the NTRA fined Telecom Egypt 20 million Egyptian pounds ($646,340) after infrastructure failure led to voice and internet service disruptions across multiple parts of the country. **52** Similarly, in March 2023, the NTRA announced that it was imposing a 20.5 million Egyptian pound ($662,500) fine on Vodafone Egypt for a partial outage in its 4G network. **53**

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 independent news websites during the coverage period as part of a wider crackdown on freedom of expression. Through Article 7 of the Law on Combating Information Technology Crimes, the National Telecommunication Regulatory Authority (NTRA) can order telecommunications companies to block websites. As of June 2024, 562 websites have been blocked in Egypt, including approximately 132 news websites. **54**

Several independent news websites were blocked during the coverage period. In June 2023, Egyptian authorities blocked both political news site Soulta 4 and Masr 360, which documents human rights violations. Both blockings were reportedly due to licensing issues (see B3 and B6); however, rights groups have speculated

that the two sites were blocked due to their published content, which at times was critical of the Egyptian government and its policies. **55**

In October 2023, the Supreme Council for Media Regulation (SCMR) announced a six-month blocking of independent website Mada Masr on the grounds that the website was "practicing media activities without a license" and "publishing false news without checking its sources." **56** The blocking came after the website published a report about Egypt's potential reception of Palestinian refugees fleeing the Israel-Hamas war in the Gaza Strip. The headline of the article was later modified (see B2). The SCMR launched an investigation into Mada Masr, and the outlet's editor in chief, Lina Attalah, also faced criminal charges (see C3).

During the previous coverage period, 12 websites were blocked on the grounds that they propagated false information, incited violence, or mocked religious beliefs, among other reasons. Additionally, some foreign-based websites were blocked for operating without a SCMR license. **57**

In November 2021, the website Disclose, a nonprofit newsroom and investigative journalism organization, was blocked after it revealed that French companies had sold surveillance systems to Egypt (see C5). **58** In July 2021, the "180 investigations" website was permanently blocked by the authorities without any stated reason or due process (see B3). **59**

Many international and local news sites are blocked, with some having been blocked since the beginning of 2017. Blocked sites include Huffington Post Arabic, financial newspaper *Al-Borsa*, and the entire online publishing platform Medium. Websites run by Human Rights Watch (HRW), Reporters Without Borders (RSF), and the April 6 Youth Movement, which was active during the 2011 revolution, are also inaccessible. **60**

In October 2020, it was reported that the Egyptian government had used Sandvine's technology to block hundreds of websites, including 100 independent news and media websites and the popular citizen news platform Al-Manassa (see C5). **61**

Despite the extensive blocking of independent news websites and those hosting human rights-focused content, all major social media platforms are readily available in Egypt. However, in August 2023, the Egyptian senate discussed

banning TikTok and "other similar applications that fail to meet the nation's safety policies and standards." Despite these conversations, TikTok remained available in Egypt at the end of the coverage period. **62**

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 and pressured social media users to take down critical content.

Streaming platforms have also been forced to remove online content. After the coverage period, in June 2024, the SCMR ordered Amazon Egypt's Prime Video platform to remove content that was deemed "inconsistent with the religious values of Egyptian and Arab societies." There were no details provided about the nature of the content in question, and Amazon Egypt removed the content within 24 hours of the request. **63**

During the previous coverage period, authorities released several political prisoners in response to growing international pressure ahead of COP27; however, at least seven released prisoners reported that the National Security Agency (NSA) ordered them to remove social media content critical of the government or face arrest at the end of the conference. Those who refused to comply were rearrested. **64**

Prepublication censorship is common. In May 2022, the Chamber of Travel and Tourism Companies and Agencies banned employees from posting social media content that could negatively impact tourism. The regulations came after two tour operators were arrested for posting a video that showed several boys harassing foreign women tourists at the Giza Pyramids. **65** Shortly before the September 2019 protests, the SCMR published an article titled "Blocking and fines are the penalty for spreading rumors in the media," reiterating Article 17 of the SCMR's Sanctions Regulations, which provides penalties for spreading false news or rumors and for inciting violations of the law. **66**

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 the authorities to censor online content, curtail freedom of expression online, and clamp down on internet users. **67** Social media content is removed following demands from the government. Progovernment lawyers have filed lawsuits against social media influencers, at times resulting in their content being deleted. **68**

In November 2020, the SCMR amended licensing regulations to pressure streaming platforms to obtain a certificate of approval for operation (see B3 and B6). The regulations also include some provisions requiring companies to remove "harmful content." Companies must comply with content removal requests within 24 hours. The SCMR is awarded discretionary power to make decisions about how to respond to noncompliance. **69**

> **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 June 2024, after the coverage period, the SCMR announced that all digital and encrypted satellite platforms must adhere to the country's content standards. While some platforms have reportedly begun compliance efforts, others have not. This directive followed concerns that content on Amazon Egypt's Prime Video platform violated the "religious values of Egyptian and Arab societies" (see B2). **70** Similarly, in September 2022, the SCMR published a statement on its website noting that streaming platforms such as Netflix and Disney+ must adhere to "the customs and values of the Egyptian state." **71**

The June 2023 blockings of Soulta 4 and Masr 360 (see B1) lacked transparency. According to Egypt's Journalists' Syndicate, both websites were blocked due to failing to obtain a license (see B6). **72** The founder of Masr 360 reported that he had applied for a license with the SCMR over six months prior to the blocking and never received a response. **73**

A May 2018 Supreme Administrative Court decision limited the ability of administrative courts to restrict executive orders for online censorship and facilitated new legislation granting judicial and executive bodies, including the NTRA, **74** the right to block websites on national security grounds. **75**

In August 2018, President Sisi signed a law to combat cybercrime and a law on media regulation (see C2). **76** The cybercrime law allows state authorities to block websites without a judicial order on national security or economic grounds, which are vaguely defined. Personnel at service providers who do not respond swiftly to blocking decisions could face prison sentences and fines. **77** The government claimed that the law was meant to combat online theft and hacking. **78** The media regulation law 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 (see B6 and C2). **79**

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. **80** Additionally, Egypt's 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. **81** The broadly worded 2015 antiterrorism law allows the authorities to block content or websites that promote terrorism. **82**

B4   0-4 pts

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

Repressive criminal laws and the rising number of arrests for social media posts have had a chilling effect on online speech. Advanced censorship and surveillance also incentivize users to self-censor and curtail political opposition on digital platforms. **83** 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.

Authorities have used legal means and blocking orders to intimidate news outlets into self-censoring. Following the October 2023 blocking of Mada Masr (see B1),

reportedly in response to an article the outlet published about the Israel-Hamas war, Mada Masr announced on its Facebook page that it had decided to modify the headline of the article in question. [84]

Recently, self-censorship has been practiced by everyday internet users, not just activists. Academics have refrained from sharing their critical opinions on social media for fear of digital surveillance or intimidation. As a result, some university professors have started educating their students on the risks of tackling certain topics on social media. [85]

A study published by the Association for Freedom of Thought and Expression (AFTE) in June 2020 found that news outlets refrain from publishing content critical of the government for fear of website blocks or further retaliation if they are already blocked. [86]

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

State officials actively manipulate information online, and the media landscape is dominated by the online versions of state-owned newspapers or outlets that are backed by government-connected individuals. [87] Journalists and bloggers face intimidation and smear campaigns from progovernment outlets. In recent years, pro-Sisi influencers have promoted government actions and policies on social media. [88]

There was some evidence of online disinformation in the lead-up to the December 2023 presidential election. Traditional and online media outlets often showed a clear pro-Sisi bias while opposition politicians were either wholly denied media coverage or were criticized. [89]

After the start of the Israel-Hamas war in October 2023, the Atlantic Council's Digital Forensic Research Lab (DFR Lab) analyzed several hashtags that were amplified by known inauthentic progovernment social media accounts. Specifically, the hashtags were accompanied by nationalist progovernment rhetoric criticizing the notion of Palestinians potentially fleeing to Sinai from Gaza.

In one case, Egyptian journalist Hossam al-Ghamry included the hashtag سيناء_خط_احمر# ("Sinai is a red line") in a post with a video of President Sisi saying, "We are not giving up Sinai for anyone, Sinai belongs to Egyptians or we die." **90**

A separate DFR Lab report published in October 2023 found that hashtags attacking Tarek el-Nabarawy, the head of the independent engineers' syndicate, were inauthentically amplified across X by progovernment accounts. The government has close ties to many syndicates and unions in Egypt, and the attacks on the head of the engineering syndicate came just before the government-aligned board made the decision to hold a no-confidence vote for el-Nabarawy. **91** In March 2024, DFR Lab also uncovered a coordinated inauthentic online campaign aimed at discrediting Ayman Hadhoud, a prominent Egyptian economist and government critic who died in custody in April 2022. The report, which analyzed Facebook and X posts going back to 2022, found that more than a dozen accounts shared identical or nearly identical social media posts that promoted unsubstantiated government claims about the events surrounding Hadhoud's death. Some of the accounts had been identified for their content manipulation efforts in other campaigns targeting Egyptian activists. **92** This pattern of inauthentic behavior is consistent with similar incidents of coordinated inauthentic online behavior reported by Twitter, now X, and Facebook in recent years. **93**

A study published in 2022 found that Egyptian authorities have launched several social media operations that used "semi-organic strategies" to attack and slander foreign adversaries. **94** In July 2021, amid Tunisia's political crisis, Egyptian media outlets, commentators, and social media influencers praised Tunisian president Kaïs Saïed's "triumph" over Ennahda—a political party in Tunisia that its opponents have linked to the Muslim Brotherhood, despite objections from Ennahda members. In Egypt, these commentators used the opportunity to launch unfounded accusations against the Muslim Brotherhood. **95**

Government agencies have sought to improve public opinion about them in the media by recruiting young Instagram and YouTube influencers to promote government policies and narratives. **96** While it is unclear whether the government is paying the influencers, some influencers have been told that their work will help boost their platforms and increase their follower counts. **97** Most

of these influencers are appointed either directly by the Ministry of Defense or indirectly as "state cheerleaders" to promote state narratives on social media. **98**

The authorities have created two WhatsApp groups to convey instructions to media outlets on what to report and what the red lines are. The first group, "Editors," is administered by the General Intelligence Service (GIS) and the second is administered by the Interior Ministry. **99**

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 such outlets have closed, and others face financial troubles. Those subjected to blocking have suffered revenue losses, leading some to suspend their operations. **100** The SCMR was created in 2016, with the power to fine and suspend media organizations. **101**

Several independent news websites were blocked for failure to obtain a license during the coverage period (see B1). For example, when Soulta 4's website was blocked in June 2023 for failure to obtain a license, it was reported that when the website's editor in chief had previously applied for a license, the SCMR requested "capital equivalent to 100,000 pounds," or approximately $3,200 (see B3). **102**

Amid the crackdown on unlicensed websites, in June 2024, the SCMR and the NTRA announced that they were "exploring technical measures to block all unlicensed platforms." Additionally, authorities ordered the Central Bank of Egypt to halt any bank transfers to platforms operating "illegally" without a license. **103**

Shortly before the December 2023 presidential elections, Saheen Masr, an independent fact-checking website, was accused by the SMRC of "violating media codes" and "international and Egyptian standards for electoral media coverage." The SMRC subsequently launched a legal investigation against Saheen Masr. Prior to the SMRC's announcement, which came just before election day, the outlet had published a report about how United Media Services, which is owned by Egypt's intelligence services, was censoring content about the election. **104**

In June 2018, the parliament approved three laws regulating the media. **105** 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 concerning 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). **106** In addition, the law requires media outlets to pay a fee of 50,000 Egyptian pounds ($1,600) to obtain a license from the SCMR and gain legal status. **107** Outlets must also have at least 100,000 Egyptian pounds ($3,200) in capital. The law allows sites to be blocked on several grounds, including spreading purportedly false news (see B3). **108**

In November 2020, the SCMR amended licensing regulations to pressure streaming platforms to obtain a certificate of approval for operation. The amendments were condemned by rights groups for being ambiguous and not specifying the fees or forms required to obtain the accreditation certificate. **109**

As of September 2021, social media influencers who earn over 500,000 Egyptian pounds ($16,150) annually are required to pay a tax to the Egyptian government. Authorities have begun reaching out to social media platforms like YouTube and Meta to get information on bloggers, influencers, and content creators who fall within this bracket. **110**

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.

B7   0-4 pts

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

Online media have 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.

Both government-affiliated and privately owned outlets have been complicit in spreading misleading information in online reporting. In August 2023, reporting from Meedan's NAWA Media Newsroom found that *Youm7*, one of the most-read news outlets in Egypt, was among the country's top promoters of misinformation. Manipulated or misleading information published by the outlet often included progovernment political propaganda that frequently praised or exaggerated government policy achievements. It was also found that many of *Youm7*'s articles relied on unverified secondary sources, or at times lacked sources altogether. [111]

The blocking of hundreds of websites has negatively affected the diversity of media and consequently of critical opinions (see B1). According to a 2018 survey conducted by Northwestern University in Qatar, only 3 percent of internet users in Egypt used virtual private networks (VPNs), which can be employed to bypass blocking and reach obstructed sites. [112] Furthermore, 54 percent of respondents in 2019 said that they feel comfortable speaking about politics, compared to 79 percent reported in 2018. Only 42 percent of respondents in 2019 believed that it is okay to express ideas online even if they are unpopular. [113]

The dissemination of fake news and misinformation adversely impacts internet users' trust of online content. During the COVID-19 crisis, fake news and false information regarding the pandemic was rampant, making it difficult for online users to access evidence-based information. [114]

B8 0-6 pts

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

Digital activism and political organizing are highly restricted. A law passed in 2013 effectively banned protests and gave the police broad powers to crack down on unauthorized assemblies. [115]

Ahead of Egypt's December 2023 presidential elections, authorities cracked down on opposition political campaigning and online mobilization activities. Ahmed Tantawi, President Sisi's most prominent potential challenger, was systematically targeted by the Egyptian security apparatus. More than 10 of Tantawi's family and friends were arrested by the security services, and his phone was infected with Predator spyware, likely also at the behest of the security services (see C5). [116] At least 73 of Tantawi's campaign members and volunteers were detained, and several faced criminal charges for allegedly "joining a subversive or terrorist group, spreading false news, and misusing social media." [117] In May 2024, an Egyptian court sentenced Tantawi and nearly two dozen of his campaign supporters to one year in prison each for their participation in a campaign, aspects of which occurred online, to collect public endorsements for Tantawi's presidential run. [118]

In April 2024, a pro-Palestinian protest was held outside the Journalists' Syndicate in Cairo. Following the protest, videos that circulated online showed one participant chanting against Ibrahim al-Organi, a powerful businessman with close ties to the Egyptian government. Al-Organi has been accused of using his companies to charge Palestinians steep fees to leave Gaza. [119] Authorities subsequently arrested 10 activists at their homes on charges of "collaborating with a terrorist group" and "spreading and publishing fake news" in relation to the video and their participation in the protests. [120] They were released a few days later. [121]

During the previous coverage period, against the backdrop of COP27, more than 150 people were detained and investigated by the Supreme State Security Prosecution (SSSP), often under "counterterrorism" charges, for using social media to organize protests. [122] The exact number of detainees remains unknown given the lack of transparency from the authorities. In addition to fines, arrests, and prison sentences, some civil society leaders have faced travel bans and asset freezes. [123]

Authorities also preemptively and arbitrarily detained several Egyptians who called for protests ahead of the climate conference. In November 2022, Mohamed Ali, an exiled former construction contractor and actor, called for antigovernment protests on social media. In response, the authorities detained dozens of activists to prevent the protest from taking place. [124] In September 2022, Gaber Mahmoud

Mahmoud Badawy was detained and held for 15 days by the security forces after calling for protests in the "11/11 Revolution - Climate Summit" Facebook group. He was accused of associating with and supporting a terrorist organization, disseminating false information, participating in a criminal conspiracy to conduct a terrorist attack, and inciting a terrorist act. [125]

Authorities frequently disrupt the work of organizations or individuals who campaign on human rights issues online. In January 2022, the Arabic Network for Human Rights Information (ANHRI) revealed that it would suspend its activities after its staff experienced "thefts, violent physical assaults, and illegal summons" following the hostile campaign by the security forces to hinder the operation of the network and its staff. [126] The ANHRI led multiple online campaigns on issues such as police reform and free expression.

In September 2019, social media users called for protests against President Sisi after corruption allegations involving the president surfaced. [127] Thousands of citizens demonstrated across Egypt, and security agents responded violently, arresting almost 2,000 people. [128] During the demonstrations, police and plainclothes security officers seized and searched the mobile devices of citizens to check for evidence of antigovernment sentiments. [129] Most of the arrested protesters were detained for being highly critical of the government online and offline. [130] Following the protests, many dissenting social media platforms were blocked (see B1). [131]

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." [132] Under Article 34, the government is given the role of preserving online security, and under Article 70

the government is responsible for regulating online newspapers and visual and radio broadcast stations. Article 71 forbids censorship 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. Article 211 outlines the establishment of a national media council tasked with regulating "the affairs of radio, television, and printed and digital press" and ensuring that the press maintains a commitment to "professional and ethical standards, as well as national security needs." [133]

In April 2019, the parliament approved amendments to the constitution that would allow President Sisi to stay in power until 2030. Among other changes, the amendments granted the president greater control over the judiciary and expanded the political and judicial authority of the military. [134] President Sisi was reelected to another six-year term in December 2023. [135]

In October 2021, President Sisi terminated the state of emergency, [136] which was first introduced in April 2017 and renewed 11 times. [137] However, numerous laws that threaten the freedom of expression, such as the 2015 antiterrorism law (see C2), remain in effect. [138] Furthermore, the government passed a number of amendments to existing legislation that permanently codify many of the provisions from the emergency law. [139]

In November 2019, a Ministry of Foreign Affairs spokesperson declared that freedom of expression is protected in Egypt, except when it targets state institutions, transcends the constitution or the 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. [140]

In September 2021, President Sisi launched the first national human rights strategy, which includes freedom of expression as a priority issue. The strategy further calls for a comprehensive code of conduct to tackle all aspects of the media, including digital and social media. [141] Egypt's Supreme Standing Committee for Human Rights issued a report in late 2022 praising the government

for its implementation of the strategy; however, rights groups have continued to document thousands of infringements on free expression. **142**

The constitution permits the trial of civilians in military courts, despite objections from political activists. **143**

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?	**O**/4

The legal framework that governs online activity restricts freedom of expression in a variety of ways. Defamation is considered a criminal offense and is included in the penal code. **144**

The 2015 antiterrorism law broadened the scope of crimes that are considered terrorism and prescribed harsh penalties for nonviolent acts. **145** Article 27 of the antiterrorism law establishes a minimum five-year prison sentence for creating a website that incites violence, hosts content that misleads the authorities on terrorism cases, or communicates with or organizes terrorist groups. **146** Activists argued that the broad language of the law could apply to any peaceful political party or advocacy group. **147** Finally, journalists face heavy fines for disputing official accounts of militant attacks. In March 2020, amendments to the antiterrorism law were passed, which prescribe severe penalties for expressing opinions online. **148** Promoting extremist ideology can carry a 10-year prison sentence, while promoting terrorist acts, extremist ideology, or ideas and beliefs that advocate violence can result in imprisonment for up to 15 years. **149**

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. **150** 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. **151** 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. **152**

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. **153**

In August 2018, the president signed the Anti-Cyber and Information Technology Crimes Law, or Law No. 175 of 2018. **154** It authorizes the blocking of websites that are deemed to be 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. **155**

Article 80(d) of the Egyptian Penal Code criminalizes the deliberate spreading of "false information or rumors" about the country's "internal conditions" with six months' to five years' imprisonment and a fine. The provision applies to content disseminated online or in print. **156** In November 2021, amid the height of the COVID-19 pandemic, the Egyptian parliament approved a bill that broadened the scope of false information by criminalizing the publication of fake news during a health crisis. **157**

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**0**/6

Internet users in Egypt operate in a highly repressive environment. **158** Those who are arrested for their online content frequently spend weeks, if not months, in pretrial detention. In an effort to bypass the Criminal Procedures Law, which outlaws the extension of pretrial detention for more than four years, authorities have embarked on a practice of "recycling defendants." **159** Many human rights activists receive renewed detentions on old or new cases. **160**

Internet users can receive long prison sentences for their online activities in cases that do ultimately proceed to trial. In January 2023, Mohamed Ali, an exiled activist whose social media posts helped fuel the 2019 antigovernment protests, was handed a life sentence in absentia for his online mobilization efforts. **161** In June

2023, student activist Moaz el-Sharkawy appeared in court after being forcibly disappeared in May. He was detained pending investigations into unsubstantiated charges of "joining and funding a terrorist group." [162] In January 2024, el-Sharkawy was further charged with "joining a terrorist group, financing terrorism, and using WhatsApp to commit a terrorist crime." The charges against el-Sharkawy could result in a life sentence. [163]

Several internet users received prison sentences for their political, religious, or social speech during the coverage period. In July 2023, Patrick George Zaki, a researcher and activist, was sentenced to three years in prison on charges of "spreading false news" after he published an online article about discrimination faced by Coptic Christians in Egypt. [164] However, following intense international pressure, Zaki was released on a presidential pardon shortly after the sentencing (see C7). [165]

In September 2023, political activist Hisham Kassem was sentenced to six months in prison after criticizing a former minister on social media. [166] In January 2024, Yahya Hussein Abdel Hadi, a former spokesperson and cofounder of the liberal Civil Democratic Movement, received a one-year suspended prison sentence for "spreading false news" after sharing several of his published opinion articles on his Facebook account. [167] Also in January, musical composer Ahmed Hegazy was sentenced to six months in prison for "contempt of religion" after he shared a video of himself singing verses of the Quran while playing an oud on social media. [168]

In October 2023, Mada Masr's editor in chief, Lina Attalah, faced charges of spreading unverified information and operating a website without proper licensing (see B1). Following an interrogation in February 2024, Attalah was released on bail of 5,000 Egyptian pounds ($160), pending further legal proceedings. [169]

In recent years, authorities have embarked on a sustained crackdown on TikTok users. In early 2023, Egyptian authorities detained five TikTok creators for sharing a popular parody video depicting a fictional visit to an Egyptian prison. They were accused of various offenses, including affiliation with a terrorist organization, financing terrorism, spreading false information, and using social media for terrorist activities. [170] In April 2023, Salma el-Shimy, a TikTok influencer with 3.4

million followers, was sentenced to two years in prison and fined $3,230 for her social media content, which promoted body positivity. **171**

Internet users are frequently arrested and detained by the state security services for posting political content on social media. In October 2023, Ahmed Sameh al-Hefnawy, a former media officer at the grassroots Tamarod Movement opposition group, was arrested and taken to the National Security headquarters, where he was blindfolded and interrogated about a video he had posted to social media. **172** It is unclear if he remains in detention. In February 2024, internet user Mohamed Ali Ahmed was arrested after sharing Facebook posts critical of President Sisi. Also in February, social media user Mohamed Atef Eid Farhat was arrested and taken to a National Security facility, where he was held for five days due to his pro-Palestinian social media posts. **173** In both Ahmed and Farhat's cases, the SSSP charged them with "joining a terrorist group, spreading false news, and misusing social media" and ordered their detention for 15 days pending further investigation. **174**

Independent online journalists were also investigated and arrested during the coverage period. In August 2023, Karim Asaad, a journalist and online fact-checker at Matsadaash, was detained for over 24 hours after publishing a report about Egyptian officials' role in smuggling cash and weapons to Zambia (see C7). **175** In November 2022, Mostafa Moussa, a freelance journalist who writes for independent news websites Masr al-Arabia and Al-Bawabh News, was arrested in Alexandria and held in pretrial detention for six months. **176** In October 2022, online journalist Ahmed Montasir was arrested and charged with spreading false news. His pretrial detention was repeatedly renewed every 15 days and his appeal was rejected in January 2023. **177**

Academics and researchers are subject to administrative, security, and judicial harassment in response to their social media content. In July 2022, an assistant professor at the Higher Technological Institute received a 15-day salary deduction after being charged with insulting the institute on social media. She was also dismissed from her position as the head of the mechanical engineering department. **178** In September 2022, Osama Rizk Rizk Amer, a teacher and YouTuber, was detained after he uploaded a video to his educational YouTube channel criticizing the process of collecting donations for both private and state

schools. Amer was held in detention for 18 days before standing trial and was charged with joining and financing a terrorist organization. [179]

Authorities continued their practice of recycling detainees by adding changes to political prisoners' cases and extending their prison sentences. Blogger Mohamed Ibrahim "Oxygen," who was initially arrested in 2018, was sentenced to four years in prison on charges of "spreading false news undermining national security" in December 2021. [180] Since at least May 2023, Oxygen has been held in solitary confinement at Badr Prison in Cairo (see C7). [181] Although his prison sentence expired in September 2023, Oxygen remained in detention as of the end of the coverage period.

Alaa Abdel Fattah, a prominent activist and blogger, was jailed for five years in 2015 and rearrested shortly after his release in March 2019. [182] In December 2021, the Misdemeanors Emergency State Security Court in Cairo sentenced him to five years in prison on charges of "spreading false news undermining national security." [183] In November 2022, after an extended hunger strike, Abdel Fattah announced he would eliminate water from this diet. [184] As of June 2024, Abdel Fattah remains in prison. [185]

During the coverage period, several political prisoners were released after serving prison sentences for their online activism or content. Ahmed Samir Santawy, an Egyptian researcher and anthropology student, was sentenced to four years in prison on charges of publishing "false news" on social media in 2021. [186] In July 2022, he received a new three-year sentence on charges of spreading false news after using social media to highlight the deteriorating situation in Egyptian prisons. [187] Following a campaign of international pressure, Santawy was released in July 2022 by presidential decree, but remains under a travel ban. [188]

Mohamed Mamdouh Abdel Halim was arrested and charged with joining a terrorist group and using social media to spread false information in 2021. He was issued a release order with precautionary measures, but the release was never carried out. [189] In December 2022, his detention was renewed by the Criminal Court for 45 days pending a second case. [190] After more than nine months in pretrial detention, Halim was conditionally released in September 2023. [191]

In September 2019, human rights lawyer and founder of the Adalah Center for Rights and Freedoms, Mohamed el-Baqer, was arrested on charges of spreading false news and misusing social media. He was later charged in a second case, for which he was neither questioned nor given the right to defend himself. [192] After spending nearly five years in detention, he was released in July 2023. [193]

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**1** / 4

Certain laws undermine the anonymity of communication in Egypt. In 2010, the NTRA issued a regulation that requires distributors of SIM cards to collect personal data from users before the cards can be activated. [194] In recent years, the NTRA has sought to remove dormant and unregistered SIM cards to promote the credibility of the Egyptian market. [195]

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 of any encryption equipment by telecommunications companies, their employees, or their customers without written consent from the NTRA and security agencies. [196] Article 72 of Law No. 180 has been criticized for granting the SCMR exclusive control over the establishment of encrypted platforms and requiring government approval for any other usage of such platforms. [197]

Encrypted messaging apps and private-chat applications are widely used in Egypt. [198] A 2022 study found that while Egyptian activists trust Signal and Telegram because of their levels of encryption, most internet users rely on WhatsApp for daily communication. [199] According to reports, Egypt's mobile app for COP27 allowed the authorities to access encrypted messages from users' mobile phones after they had registered on the app. The app also provided the MCIT with other backdoor privileges, such as the ability to scan people's devices (see C5). [200]

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 be monitored or confiscated by judicial order. 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. [201]

Egypt's cybercrime law (see C2) provides national security agencies access to the electronic data of internet and communications platforms users without judicial oversight or clear regulation. Additionally, it does not include any substantial means to mitigate privacy violations or provide for any compensation for those affected by these violations. [202]

A provision of the antiterrorism law allows the police to monitor internet traffic and social media activity to "prevent their use for terrorist purposes." [203] 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).

Privacy and surveillance concerns have been flagged around ongoing plans for the New Administrative Capital (NAC), which will be equipped with advanced surveillance systems, including facial recognition technology. [204] Furthermore, the city's mobile app, which will allow residents "to make utility payments, access public services, and register complaints with the authorities," could infringe upon the privacy of residents given the lack of data protection safeguards. [205]

Egypt's mobile app for COP27, which was meant to provide participants with information about the conference, had concerning privacy implications. According to cybersecurity experts, the app could listen in to conversations, read private emails, track texts, and bypass encryption (see C4). [206] The app requested users to register using personal information, such as their email, mobile number, nationality, and passport number, and required location tracking to be turned on. [207]

Egyptian authorities have access to spyware technology, which has been used to target journalists, activists, and opposition politicians. Between May and September 2023, Ahmed Tantawi, Sisi's most prominent potential challenger ahead of the December 2023 presidential elections, was targeted with Cytrox's Predator spyware. Tantawi's mobile phone was infected with Predator, which allowed attackers to access his device's microphone, camera, contacts, and text messages. **208** Reporting by Canadian internet watchdog Citizen Lab found that Tantawi's phone was likely infected after Vodafone Egypt's network redirected him to a malicious website where Predator was then installed. Citizen Lab reported that the attack on Tantawi could be attributed to the Egyptian government with high confidence due to the Egyptian authorities' track record as a Cytrox client and history of using Predator spyware to target members of the political opposition. **209**

In December 2021, Citizen Lab reported that, while living in exile, both opposition politician Ayman Nour and a well-known Egyptian journalist were targeted by Predator spyware. According to Citizen Lab, there is medium-high confidence that the hack was carried out by the Egyptian government, which is a confirmed Cytrox customer. **210**

In November 2021, investigative website Disclose reported that French companies Nexa Technologies, Ercom-Suneris, and Dassault Systèmes supplied the Egyptian government with a cybersurveillance system that was deployed to monitor the electronic devices of human rights organizations and activists. **211**

Other reported instances of government-linked spyware use in recent years have included the use of Sandvine devices to block websites and monitor, prevent, or tamper with connections; **212** FinSpy attacks against human rights activists; **213** and the use of other sophisticated spyware that enabled attackers to read emails, log contacts, and record locations of citizens (see C8). **214**

In February 2024, the United States Department of Commerce prohibited Sandvine, a Canadian software company, from working with American partners due to evidence that Sandvine's technology has been employed for "mass-web monitoring and censorship" in Egypt. According the US Department of Commerce, Sandvine's tools have been used by Egyptian authorities to suppress dissent and to facilitate censorship (see B1). **215**

As early as 2013, Egyptian authorities were reported to be using software that allows service providers to monitor the behavior of internet users as well as a wide range of communications, including voice calls, text messages, emails, instant messages, social media platforms, and search engines. [216]

Police and plainclothes security agents have also searched and seized mobile devices (see B8). [217] Amid the call for protests in November 2022, checkpoints were set up where people had to unlock their phones and allow the authorities to inspect their social media apps for any political content. It was reported that some officers used advanced digital tools when searching mobile phones, including to detect hidden applications. [218]

In 2019, the Public Prosecution established the Communication, Guidance, and Social Media Department (CGSMD), which has a Monitoring and Analysis Unit (MAU) dedicated to monitoring social media users. The MAU has filed several lawsuits against social media users (see C3). [219]

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 personal data from users. It also compels providers to give security agencies access to their "equipment, systems, software, and communication." [220]

The 2018 cybercrime law requires telecommunications providers to assist law enforcement with surveillance operations. The law also compels providers to collect personal data and store it for 180 days. [221] Failure to retain data for this amount of time could result in a fine of up to 10 million Egyptian pounds ($323,000); a second violation can lead to a fine of 20 million pounds ($646,000) and the revocation of the company's license. [222] State agencies can request stored data without a judicial order, [223] an apparent violation of Article 57 of the constitution. [224]

A data protection law ratified by the president in July 2020 is the first legal safeguard for individual data privacy, and contains some data protection principles. [225] However, the law stipulated that service providers should retain users' data for 180 days and provide access to state authorities upon request. [226] Furthermore, it exempts national security authorities from user data protection obligations. It also fails to guarantee the independence of the Personal Data Protection Center, which will serve as the regulatory authority. [227] As of June 2024, the law has not been fully implemented and relevant authorities have yet to finalize the legislative framework or establish the necessary bodies to enforce the law. [228]

In May 2018, the parliament passed a law to regulate ride-sharing apps, [229] which includes requiring companies to retain user data for 180 days and share it with authorities "on request" and "according to the law." [230] Requests for data do not need to be accompanied by a warrant, though a decree from the prime minister is required. [231]

Google's most recent transparency report, covering the second half of 2023, revealed that Egyptian authorities made two emergency disclosure requests for user information during that period. [232] Facebook also reported receiving twelve requests from the government for user data from 14 accounts during the same period. [233]

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. Enforced disappearances and kidnappings of online activists and journalists are not uncommon. [234] Prison authorities and security forces operate with impunity and often face no repercussions for these abuses. [235]

In August 2023, Egyptian security forces raided the home of Karim Asaad, a journalist for independent media platform Matsadaash, physically assaulted Asaad and his wife, and threatened to harm their two-year-old son. During the raid, security forces also seized all cell phones from the home as well as jewelry and

8,000 Egyptian pounds ($258) in cash. Asaad was arrested, likely in retaliation for two Facebook posts published on Matsadaash's page, which security forces deleted after logging into the outlet's account. He was denied access to legal representation and released a day after the raid. [236]

Family members of exiled government critics or dissidents living abroad face legal harassment. In August 2023, Gamal Ziada, a tailor and the father of critical journalist Ahmed Gamal Ziada, was arbitrarily detained on charges including "spreading fake news," "harmful use of social media," and "membership of a subversive organization." According to rights groups, Gamal Ziada's arrest appeared to be in retaliation for his son's role as editor of Zawia Thalitha, an independent investigative website based in Belgium. Ahmed fled Egypt in 2019 after facing threats and repeated arrests in response to his online journalism. Gamal Ziada was released from detention a month following his arrest. [237]

Social media users have been forcibly disappeared by security forces in the past. In June 2022, a student, Al-Amir Fahim Ahmed, posted a video on TikTok in which he performed a political song called "Theaters and Cinemas." After posting the video, he was forcibly disappeared for more than a week before being formally arrested and investigated by the SSSP (see C3). [238] In January 2022, Ihab Saeed Ahmed Saafan, an accountant, was forcibly disappeared for around three weeks. Saafan, who was accused of "joining and financing a terrorist group" and "spreading false news," reported being beaten and subjected to electric shocks while security forces interrogated him about his Facebook and Twitter posts. [239]

Torture and abuse in prisons is not uncommon. Blogger Mohamed Ibrahim "Oxygen," who has been held in prison since 2018 (see C3), began his second hunger strike in April 2024 to protest his extended detention, citing "mistreatment, abuse, and [...] unsanitary conditions." Rights groups have reported that Oxygen has been denied access to medication and has suffered psychological issues after spending extended periods of time in solitary confinement. [240]

In February 2020, Patrick George Zaki was detained for 24 hours by Egyptian authorities. 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. [241] While in custody, Zaki was

subjected to torture, including electric shocks. In July 2023, Zaki was granted a presidential pardon just one day after receiving a three-year prison sentence for spreading false news (see C3). **242**

Online gender-based violence is common in Egypt, and women routinely face online harassment and hate speech. In August 2023, Aya Mounir, a feminist content creator and founder of the Superwomen Initiative, reported that she has routinely been targeted with misogynistic insults and threats of violence on social media after sharing feminist content online. **243**

Online harassment and doxing of LGBT+ people is common, **244** and evidence shows that authorities have relied on cyberinformants to identify and arrest sex workers and members of the queer community since the early 2000s. **245** In March 2023, LGBT+ dating app Grindr sent a cautionary message to its Egyptian users after reports emerged that Egyptian authorities were using the app to identify and arrest members of the LGBT+ community. **246** Throughout 2022, Human Rights Watch (HRW) observed a trend of digital repression by security forces against LGBT+ people. **247** Specifically, the cybercrime law was used to arrest LGBT+ people, allegedly due to digital evidence found on their personal devices. Detainees also reported that they were treated poorly while in police custody. **248**

During the previous coverage period, National Media Authority staff members were threatened by officials in response to their critical social media posts. One staff member had his salary suspended for five days after using social media to condemn a 2006 proposal by a parliamentarian to halt broadcasting of various regional channels. Other staff were reportedly suspended from work and their salaries were suspended without any legal or administrative investigations. **249**

C8   0-3 pts

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

Internet users in Egypt have been subject to several internal and external cyberattacks in recent years. **250** According to a May 2023 report from Kaspersky,

international hacking teams who specialize in advanced cyberattacks targeted Egyptian government institutions with the intent of espionage and data theft. [251]

Private companies and individuals were targeted by cyberattacks or with malware in recent years. In November 2022, hackers obtained the WhatsApp numbers of 45 million Egyptian citizens, which were then sold online. [252] In early 2022, reports emerged that thousands of Egyptian internet users had been infected with RedLine Stealer malware. The malware is used to steal passwords, credit card information, and other sensitive data. [253]

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. [254]

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. [255]

Footnotes

1   Simon Kemp, "Digital 2024: Egypt," Data Reportal, February 23, 2024, https://datareportal.com/reports/digital-2024-egypt

2   Simon Kemp, "Digital 2024: Egypt," Data Reportal, February 23, 2024, https://datareportal.com/reports/digital-2024-egypt

3   Egypt Ministry of Communication and Information Technology, "ICT Indicators in Brief - January 2024 Monthly Issue," February 2024, https://mcit.gov.eg/Upcont/Documents/Publications_462024000_ICT_Indicat ...

4   Portulans Institute and Oxford Saïd Business School, "Network Readiness Index 2023 – Egypt," November 20, 2023, https://networkreadinessindex.org/country/egypt/

5   "Egypt," Speedtest Global Index, Accessed June 2024, https://www.speedtest.net/global-index/egypt

More footnotes

On Egypt

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

See More ›

Country Facts

Population

111,000,000

Global Freedom Score

18/100   **Not Free**

Internet Freedom Score

28/100   **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

Other Years

2023

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

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

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org