Freedom House

FREEDOM ON THE NET 2024

Saudi Arabia

NOT FREE

25 /100

A. Obstacles to Access	13 /25
B. Limits on Content	7 /35
C. Violations of User Rights	5 /40

LAST YEAR'S SCORE & STATUS

25 /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

Saudi Arabia continued to rank as one of the world's lowest-scoring countries on internet freedom. Internet users in the kingdom faced extensive censorship and surveillance as well as limited access to diverse content, and users who criticized the government remained subject to persecution, with some receiving multidecade prison sentences for peaceful online expression.

- Online accounts that were aligned with the government led coordinated smear campaigns and other attacks against media outlets and individuals (see B2 and B5).
- A women's rights activist was sentenced to more than a decade in prison, and was reportedly tortured in custody, resulting in a broken leg (see C3 and C7).
- Users received multidecade prison sentences for their social media content, and one received a death sentence for his online activity (see C3).

Political Overview

Saudi Arabia's absolute monarchy restricts almost all political rights and civil liberties. No officials at the national level are elected. The regime relies on extensive surveillance, the criminalization of dissent, appeals to sectarianism and ethnicity, and public spending supported by oil revenues to maintain power. Women and members of religious minority groups face extensive discrimination in law and in practice. Working conditions for the large expatriate labor force are often exploitative.

A. Obstacles to Access

A1 0-6 pts

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

Rapid growth in internet and communication technologies (ICTs) has produced robust infrastructure and widespread internet access throughout the country. At the start of 2024, there were 36.84 million internet users in Saudi Arabia, resulting in an internet penetration rate of 99 percent. [1] Mobile usage is also widespread; there were more than 49.89 million mobile connections as of February 2024, according to the data aggregator DataReportal. [2] Approximately 99 percent of the population is covered by at least fourth-generation (4G) mobile networks, according to the Ministry of Communications and Information Technology (MCIT). [3]

The government continues to invest heavily in the ICT sector as part of its Vision 2030 reform program. The country ranked third in the Middle East for availability of fifth-generation (5G) mobile service, according to OpenSignal's Global 5G Benchmark, published in June 2023. The report found that Saudi Arabia has achieved 23.5 percent 5G availability across the country. [4] In 2022, the government signed memorandums of understanding with the US government on the advancement of 5G and 6G rollouts, [5] and with China's Huawei Technologies on cloud computing and the building of high-tech complexes. [6] Cloud regions have also recently expanded into Saudi, with Microsoft, AWS, and Google announcing cloud regions during the coverage period. [7] Mobile service providers Saudi Telecom Company (STC), Zain, and Mobily also continued 5G expansion programs during the coverage period. [8]

Internet speeds are fast and reliable. [9] As of December 2022, Saudi Arabia ranked fifth out of 130 countries for median mobile internet connection speed, according to a joint report by Boston Consulting Group and Meta. [10] However, a large number of Saudi internet users report experiencing far lower mobile broadband speeds than what is quoted to them by their providers—including STC and Mobily. Many customers have conducted independent internet speed checks and found that the speed does not match what they are paying for as part of their internet packages. [11] According to Ookla's speed tests in April 2024, the median mobile download and upload speeds stood at 117.12 megabits per second (Mbps) and 13.96 Mbps, respectively. The median fixed-line broadband download and upload speeds stood at 110.04 Mbps and 54.16 Mbps, respectively. [12]

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

While internet and mobile services are relatively expensive by global standards, they are affordable for a majority of people living in Saudi Arabia.

According to the United Kingdom–based firm Cable, the average monthly cost of consumer broadband services in 2024 was $91.53, up from $88.32 in 2023. [13] In 2023, the average cost of 1 gigabyte (GB) of mobile data was $1.49. [14] The average annual salary in Saudi Arabia is around 101,296 riyals ($27,000), which is equivalent to a monthly salary of 8,400 riyals ($2,200). [15] Significant wage gaps exist between men and women, government and private-sector employees, and nationals and foreigners working in Saudi Arabia. [16] These income disparities present obstacles to access for disadvantaged socioeconomic groups. [17]

Rural villages and provinces—home to about 15 percent of the population in 2023, according to the World Bank [18] —have historically had poorer internet connectivity compared with urban metropolitan areas. [19] However, the government and major service providers have continued efforts to improve connectivity in these regions. As of the first quarter of 2023, 97 out of the country's 136 governorates had access to 5G coverage. [20]

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 exercises technical control over internet infrastructure for the purpose of restricting connectivity.

Regulators and telecommunications companies have historically taken an aggressive stance against free or low-cost Voice over Internet Protocol (VoIP) services that potentially reduce the amount of standard mobile calls, circumvent the associated regulatory framework, and sometimes bypass the government's surveillance apparatus. Internet service providers (ISPs) and the industry regulator, the Communications, Space, and Technology Commission (CST), have

previously blocked VoIP applications including Viber, [21] WhatsApp, [22] and FaceTime, [23] as well as integrated chat systems on social media platforms such as Facebook Messenger. [24] A study released in 2020 found that nearly all messaging services were accessible in the country, except for WhatsApp, though some user experiences differed. [25] As of June 2024, most VoIP services—apart from WhatsApp—were available. [26]

While the reasons behind the historical blocking of VoIP services have never been formally disclosed by either Saudi authorities or providers, local observers are of the opinion that the practice was driven by a combination of protectionary measures on behalf of service providers, financial and security concerns, and an attempt to limit encrypted communications (see C4). [27]

Saudi Arabia is connected to the internet through two country-level data service providers, Integrated Telecom and Bayanat al-Oula for Network Services. The servers they utilize are split between the state-owned internet backbone and global servers. All user requests that arrive via Saudi ISPs travel through these servers, making them subject to censorship at a centralized point. [28]

A4 0-6 pts

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

The two country-level service providers offer services to licensed ISPs (see A3). Most fixed-line broadband and mobile services are provided by three long-established companies: STC, Mobily, and Zain. Smaller groups also operate, including companies headquartered abroad, such as Virgin Mobile. As part of its overall economic and social reform strategy, the government has streamlined laws to attract foreign firms, including cloud-computing and technology-service providers, and has eased foreign-ownership rules and other regulatory hurdles.

A new Telecommunications and Information Technology Act (TITA), adopted by royal decree, came into force in December 2022 (see A5). The TITA aims to encourage competition between ICT service providers, in part by requiring controlling service providers—those with over 40 percent of the relevant market share—to meet interconnection and accessibility requests on "fair" terms and prices and according to CST-approved costs. Language in the TITA also aims to

prohibit dominant providers from abusing their position. [29] The decree came after a series of complaints that major service providers were engaging in unfair trade practices. [30]

Certain barriers to market entry remain. For example, new entrants are required to work under a prelicensed local operator. [31] According to the TITA, the CST board may require a license or registration for providing specific ICT services or creating special telecommunications networks. [32]

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

The CST is responsible for regulating the internet. [33] Its board of directors is headed by the communications minister, who, like all cabinet members, is appointed by the monarch. [34] There are no explicit guarantees protecting the CST from political or commercial interference.

Among its provisions, the 2022 TITA states that the CST must approve any material change of ownership of a licensee or registered telecommunications provider (see A4). It also widens the scope of the CST's jurisdiction, requiring the commission's approval for any use of telecommunications networks, which could include regulation of "over-the-top" services. [35]

The CST regularly imposes fines on service providers. However, specific information on the nature of infractions is rarely provided, making it difficult to judge the merit of any penalties.

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

Authorities block a wide range of websites under rules prohibiting content that is deemed harmful, illegal, anti-Islamic, or offensive. Criticism of the Saudi government, its policies, or its regional allies is not tolerated, online or otherwise.

News websites that publish critical content about the government are blocked. These include the London-based online news outlet Middle East Eye as well as the website of London-based newspaper *Al-Araby al-Jadeed* and its English-language affiliate *New Arab*, which has been blocked since January 2016. [36] Some Qatari, Iranian, and Turkish news sites have been blocked amid political tensions between those countries and Saudi Arabia. [37] Turkish outlets, such as the state-run Anadolu Agency, were finally unblocked in May 2022 when the two countries resumed diplomatic relations. [38] News sites with views that oppose the Saudi government or its geopolitical and strategic aims are also blocked, including the website of Beirut-based broadcaster Al-Manar, which is owned by the Iranian-backed Lebanese militant organization Hezbollah, and websites run by Yemen's Houthi rebel movement, which Saudi armed forces actively fought for more than seven years beginning in 2015. [39] The websites of Democracy for the Arab World Now (DAWN), a US-based nonprofit advocating for greater rights in the Middle East, as well as Al-Estiklal, an Arab dissident news platform, are similarly blocked in Saudi Arabia. [40]

The government routinely blocks websites disseminating violent extremist content, as well as those related to pornography, gambling, illegal drugs, and unauthorized use of copyrighted materials. [41] The Saudi Authority for Intellectual Property blocked 3,317 websites over copyright breaches in 2023. [42]

Websites and social media pages belonging to human rights or political organizations, such as Avaaz and the National Assembly Party, a political party founded by Saudi dissidents abroad, are blocked. [43] LGBT+ content is also widely blocked. A 2021 report by the Open Observatory of Network Interference (OONI) found that Saudi Arabia has the world's highest percentage of LGBT+ "website blocking consistency." According to the report, Saudi ISPs have used WireFilter censorship technology to block specific web pages. WireFilter, which was developed by the Riyadh-based company Sewar Technologies, is a network-filtering system designed for service providers and other commercial entities. [44]

Popular social media and communication applications are not consistently blocked, though users have reported that Clubhouse is banned, despite the lack of a formal blocking statement from the government. [45] Several platforms' VoIP services have been intermittently blocked by authorities in the past (see A3).

Saudi internet users regularly use circumvention tools such as Hotspot Shield, which allow them to bypass censorship through virtual private networks (VPNs). [46] However, the websites of Tor and other major VPN providers are blocked by the government. [47]

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

Blocking and filtering by authorities is complemented by state and nonstate censorship and forced content removal. Outlets frequently delete user-generated content that could be deemed inappropriate or inconsistent with societal norms, as they can be held liable and face legal penalties for content posted on their platforms (see B3). [48] As a result, it is unusual to find antigovernment comments on the websites of major Saudi newspapers, which do not reflect the diversity of political views seen on social media. In early 2024, Thamanyah, a Saudi media company, launched a new digital platform hosting Arabic-language podcasts. [49] The platform was quickly attacked by progovernment social media accounts for hosting content that they deemed politically offensive to the country, leading it to remove the relevant channels. [50]

Saudi dissidents and political activists who post content that is critical of the Saudi government from outside the country have reported incidents in which platforms like Facebook and X (known as Twitter until 2023) have removed content or blocked access to their accounts. [51] In February 2021, *New Lines Magazine* reported that women who published content recounting their experiences in Dar al-Reaya—a network of detention centers for women in need of "social correction"—had their videos taken down. [52]

In July 2022, the CST and the General Commission for Audiovisual Media (GCAM) requested that YouTube remove "inappropriate ads" that they said contradicted Islamic values and broke Saudi media laws. They threatened legal action should the platform not comply with their request. [53] No action by either party appeared to have been taken as of June 2024. [54]

In January 2024, the CST approved its Regulations for Providing Digital Services, a regulatory framework for digital content. The regulation requires local and international service providers to apply for a license, registration, or notification from the CST. Online audio and video streaming platforms as well as social media companies must comply with all CST requests, including potential content removal and data requests in line with the "applicable law in the Kingdom." The regulation also imposes further financial and regulatory implications for online service providers and content hosts (see B6). [55]

In September 2022, Saudi Arabia joined five other Gulf Cooperation Council (GCC) countries in a joint statement calling on Netflix to remove content that they claimed "violates Islamic and societal values and principles." The countries reportedly threatened legal action if Netflix failed to comply. [56] Though the content in question was not specified, local media and officials in the six countries had criticized Netflix for programming that showed same-sex relationships or allegedly portrayed children in a sexualized manner.

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

No comprehensive list of sites banned by the authorities is publicly available. In certain cases, users who attempt to access a banned site are redirected to a page displaying the message, "Access to the requested URL is not allowed!" A green background is displayed on CST-blocked sites, whereas sites blocked by the Media Ministry for licensing violations or copyright infringement have a blue background. However, several blocked sites also return a generic "this site can't be reached" error message. [57] A 2020 digital-filtering study found that most filtering was based on HTTP filtering, augmented with transport layer security–level filtering for HTTPS connections. [58] In September 2023, a draft Global Digital Content Safe

Harbor Law was introduced. This is the first intermediary liability law for global digital content in the kingdom. While the law includes an immunity principle for intermediaries in relation to third-party content, vague language leaves loopholes to this principle. For example, the intermediary is protected if the intermediary service includes global digital content, but it is unclear if the protection applies to local digital content providers. To be exempt from intermediary liability, companies must also apply for a certificate with the CST, which can be canceled, suspended, or not renewed. [59] These conditions may prompt platforms to monitor and remove more content to avoid being penalized (see B2).

The government receives blocking requests from members of the public, who can use a web-based form to submit a complaint regarding "undesirable" material. [60] Once an individual submits the form, a team of CST employees determines whether the request is justified. [61]

Data-service providers must block all sites banned by the CST, [62] and failure to abide by these bans may result in a fine of up to 25 million riyals ($6.7 million), according to Article 38 of the Telecommunication Act. [63] However, social media platforms have been blocked without an official ban released by the CST, as was the case with Clubhouse (see B1).

The CST provides "filtering lists to data-service providers to apply on internet gateways." [64] The commission does not provide further details on these lists.

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**0** / 4

Online self-censorship is pervasive. Social media users are extremely cautious about what they post, share, or "like" online due to the threat of harassment or prosecution under broadly worded antiterrorism and other laws. Users who express support for liberal ideals, the rights of minority groups, or political reform, in addition to those who expose human rights violations or otherwise scrutinize government policy, are closely monitored, and they are often targeted for reprisal by the government (see C5).

Repression of free speech has worsened in recent years, motivating greater self-censorship in even private communications on topics like the actions and policies of individuals within the crown prince's inner circle. [65] In 2022, the executive director of DAWN stated that the level of fear being experienced by Saudi citizens was "unprecedented" given the consequences for voicing any criticism or "objection to anything that [Crown Prince] Mohammed bin Salman is doing" (see C3). [66]

The threat of imprisonment, coupled with the risk of being labeled a traitor by progovernment media outlets, [67] has also led journalists and activists to self-censor (see C3). [68] Several Saudi journalists stopped writing for local media outlets for fear of breaching government redlines, according to interviews conducted in 2020. [69] Some of these journalists described parameters of acceptable public discourse that constantly fluctuate, as well as feeling direct and indirect pressure to publish content praising the government's policies. [70]

Foreign correspondents have cited difficulties in obtaining quotes or information from Saudi industry professionals, including economists, on issues like unemployment. On several occasions, journalists for international news outlets have had interview requests denied on the basis of their outlets being "too negative" about Saudi Arabia. [71] Saudi-based journalists and online commentators continue to feel increasing pressure to censor their content, or avoid particular topics entirely, given the risk of provoking the government. [72]

Questioning religious doctrine is strictly taboo, particularly any content related to the prophet Muhammad. Saudi women have often been pressured to refrain from posting photos of their faces online, and many continue to be discouraged by their families from disclosing their names online, leading them to use pseudonyms instead. Some women have faced repercussions from family members, including physical abuse, for flouting such moral constraints. [73]

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?	**0** / 4

The government controls news outlets across all media, including in the digital sphere. Moreover, officials use a variety of online tactics to create an illusion of popular support for government policies at home and abroad.

Critics suspect that the government employs an "electronic army" to promote progovernment views, particularly on social media. Progovernment trolls have taken to "hashtag poisoning," in which a popular hashtag—on a platform like X—is flooded with unrelated or opposing posts so as to disrupt criticism or other unwanted conversations. **74**

The University of Oxford's Computational Propaganda Research Project concluded in 2019 that government actors employ permanent staff to spread disinformation and propaganda. The same report noted that Saudi Arabia was named by Facebook and Twitter as one of seven countries that used their platforms to "influence global audiences." **75** Activists and journalists have identified "entire Saudi-based marketing firms" dedicated solely to running inauthentic accounts for the Saudi government. **76** In October 2023, the Atlantic Council's Digital Forensic Research (DFR) Lab reported that a network of anonymous progovernment X accounts launched a coordinated call to reinstate the account of Saud al-Qahtani, a former adviser to the crown prince who was accused of orchestrating the 2018 murder of journalist Jamal Khashoggi and has been banned from X since 2019. **77** Hatice Cengiz, Khashoggi's fiancée, has received online harassment and death threats from progovernment X accounts. **78**

In January 2023, rights groups DAWN and the Social Media Exchange (SMEX) published a joint statement claiming that the Saudi government had recruited Saudi-based Wikipedia administrators in an effort to control online information about the country. In September 2020, Saudi authorities imprisoned two well-known Wikipedia administrators, Osama Khaled and Ziad al-Sufyani, for reasons that were unclear. **79**

After the coverage period, hundreds of Muslim pilgrims died during the July 2024 Hajj season in Mecca due to extremely high temperatures. Many of the deceased made their pilgrimage without the proper registration, often because of the associated costs, which meant that they had limited access to public facilities and transportation. Progovernment influencers have reiterated the message that the

deaths resulted from lack of proper registration, absolving the Saudi government of its responsibility to provide adequate care to Hajj pilgrims. The government supporters went on to circulate a hashtag, #وفيات_الحج_ضحيه_دعاه_الفتنه (#HajjDeathsAVictimofSeditionPromoters), blaming foreign religious leaders for supposedly encouraging people to perform the Hajj without a permit. Civil society organizations have responded with a #الحج_ليس_آمناً (#HajjIsNotSafe) campaign, calling on the Saudi government to take responsibility for the tragedy. [80] Meanwhile, an Egyptian pilgrim was detained after posting a video in which he criticized the negligent conditions and lack of medical services that contributed to the deaths. [81]

The government has invested in online outlets that help promote its preferred narratives among foreign news organizations. This includes partnerships between the Saudi Research and Marketing Group (SRMG), the country's largest publisher, which has links to the royal family, and international media companies such as Bloomberg and the London-based Independent news group. After concerns emerged over the SRMG's level of editorial influence within Bloomberg, the outlet reduced the scope of the partnership. [82] Vice, a Canadian-American media outlet, has partnered with the MBC group, a media company that is majority owned by the Saudi government. Several Vice reporters have stated that their content, especially material that was critical of Saudi human rights violations, was removed or had its publication postponed, allegedly due to concerns about repercussions for Saudi-based staff. [83]

The government regularly invites online influencers to visit Saudi Arabia on all-expenses-paid trips, with the apparent aim of persuading them to disseminate an idealized vision of the country. [84] Separately, digital rights advocates say there is a need for greater scrutiny of the government's online human rights violations, disinformation campaigns, and influence operations in light of the kingdom's position as X's second-largest source of investment. [85]

Automated social media accounts have been used to manipulate the online narrative around several regional events, often pushing progovernment positions. In July 2021, reports indicated that a surge of social media propaganda from Saudi Arabia was portraying Tunisian president Kaïs Saïed's undemocratic decision to suspend the parliament and dismiss the prime minister as a popular revolt against the Muslim Brotherhood. [86] Following the Russian regime's full-scale military

invasion of Ukraine in February 2022, a group of online trolls originating in Saudi Arabia and the United Arab Emirates (UAE) spread Russian disinformation about the war. [87]

Progovernment commentators frequently smear government critics online. For example, Hussain al-Ghawi, a progovernment online commentator, has played a key role in multiple online attacks that were circulated or amplified by a network of progovernment nationalists, bots, and inauthentic accounts, including a campaign against Khashoggi in the months preceding his death. [88]

The government frequently issues warnings and directives to reporters, internet users, and others. The threat of hefty fines and prison sentences is employed to discourage internet users from publishing information deemed by authorities to be contrary to "public order" (see C2 and C3). According to the *Economist*, for example, clerics and preachers have been banned from posting "anything but praise" on social media for the actions and achievements of Crown Prince Mohammed bin Salman. [89]

B6 0-3 pts

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

Online and print outlets cannot operate without explicit approval from the highest levels of government. [90] The Media Ministry stipulates licensing requirements for those seeking to publish online. Article 7 of the Regulations for Electronic Publishing Activity requires applicants to be Saudi nationals, at least 25 years old, university graduates, of "good conduct," and not employed by the government. Article 15 prohibits publishing anything that contravenes Islamic law, violates public order, or serves "foreign interests," as well as any material that incites a "spirit of discord" within society. [91]

A draft media law was proposed in November 2023 by the General Authority of Media Regulation (GAMR). It was intended to overhaul the existing legal frameworks regulating the media, including digital communications platforms and social media, and established GAMR as the entity responsible for issuing and renewing required licenses. Digital platforms would also need a license to conduct media activity, including creating, disseminating, or streaming media content. Civil

society organizations have expressed concern that the draft law would only worsen censorship of the media by extending its excesses to social media accounts. [92]

In September 2022, the GCAM introduced "Mawthooq," a new protocol requiring individuals to obtain an official license to advertise on social media. [93] This applies to any content creator who earns revenue through online marketing, such as social media influencers. [94] As part of the new regulations, the GCAM announced that non-Saudi residents or visitors to the country would be prohibited from posting advertisements on social media unless they held a license authorizing them to do so and worked within an established commercial entity. Those who violate this rule would face a five-year prison sentence and fines of up to $1.3 million. The relevant license comes at an annual cost of roughly $4,000. [95] The government can also request that advertisers cancel ads on a particular website to pressure it to close.

Under the CST's Digital Content Platform Regulations, approved in January 2024, video over-the-top (OTT) platforms and audio on-demand platforms with a certain number of subscribers would be required to pay annual fees of 50,000 riyals ($13,000) (see B2). [96]

B7 0-4 pts

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

The government blocks a wide range of websites and can order the removal of content, limiting the diversity of the online information landscape (see B1 and B2). Existing news sources in Saudi Arabia largely offer the same narratives and views —in line with those of the government—given that dissenting voices are frequently censored. [97] Independent media outlets, both offline and online, are nonexistent within Saudi Arabia. [98]

While opposition blogs and online forums were once the main venues for discussing political and social matters, such discussions now take place on social media, as the use of platforms like X and Snapchat continues to grow. [99] Opposition figures abroad use YouTube, Snapchat, and X to distribute content, partly because their websites are blocked within the country. [100] However,

pressure on users to self-censor remains high, and the fear of arbitrary arrest has increased as speech interpreted as critical of the authorities becomes more likely to draw punishment (see B4). [101] Consequently, journalists and online commentators can only safely present a progovernment narrative.

Some Saudi dissidents have warned that the government's monitoring of X has limited the platform's utility for open discussion (see B5). [102] Within the country, scholars note that X previously served as a popular platform for debate, but has since fallen under effective government control, [103] resulting in significantly muted debate among users and the outright abandonment of the platform by others. [104] Local commentators have underscored a similar trend with the audio-chat application Clubhouse, which gained popularity among Saudi users in 2021. Saudis have said they are reluctant to join conversations hosted by dissidents for fear of monitoring by state intelligence services (see B1 and C5). [105]

The English-language websites of most international news agencies are available. Arabic content is also widely available, as are Arabic versions of commonly used social media sites and mobile applications. Online spaces for certain minority groups, such as LGBT+ people, are largely unavailable.

Saudi internet users regularly employ VPNs to access websites, including blocked foreign media outlets. [106]

B8 0-6 pts

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

In the past, Saudis used digital activism to express public concerns and grievances. These online campaigns, which proliferated most widely on X, often mobilized diverse groups of constituents, though the leading participants were typically young people. During recent coverage periods, however, the government has intensified repression of political and social speech, leading to increased self-censorship and fewer opportunities for online mobilization (see B4 and C3). [107]

A number of reports have indicated that the Saudi government actively works to curb pro-Palestinian sentiment on social media. For example, after a local soccer club deleted an image of a player wearing a Palestinian keffiyeh, [108] users who

shared the post or objected to the content removal soon posted nearly identical apologies, which some observers have interpreted as a sign of government pressure. [109]

Authorities have imprisoned prominent social media users for their political, social, or religious online activism. In January 2023, it was reported that reformist cleric Awadh al-Qarni, who used social media platforms to express religious and political views to his large following, was facing a possible death sentence for spreading material that was deemed "hostile" to the country. [110] Such harsh sentences serve as a reminder to Saudi nationals and residents of the risks associated with using social media to mobilize, campaign for, or voice dissent (see C3). [111]

Saudi Arabia's restrictive laws and severe criminal penalties can reduce participation in civic mobilization efforts online. The authorities have arrested Saudi women's rights activists who used social media to protest the male guardianship system or a ban on women driving. [112] While recent legal reforms have reduced the scope of the guardianship system, the driving ban was lifted in 2018, and a number of activists have been released, some remain subject to travel bans and other restrictions. [113]

Freedom of assembly is not respected, and the government has imposed harsh punishments on those who call for public protests, both online and offline (see C2). [114]

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

Saudi Arabia has no constitution. The 1992 Basic Law, which the government states is based on the Quran and the life and teachings of the prophet Muhammad, serves as a constitutional framework.

The Basic Law contains language that calls for freedom of speech and of the press, but only within certain boundaries. The Law of Print and Publication largely consists of restrictions on speech rather than protections. [115] Online journalists employed at newspapers and other formal news outlets maintain the same rights and protections as print and broadcast journalists and are similarly subject to close government supervision (see B7). [116]

The Personal Status Law, which was published in March 2022, has been criticized for its potential to further restrict women's ability to speak freely about challenges during divorce proceedings or the country's guardianship rules (see B8). [117]

Judges have significant discretion regarding how they interpret Sharia (Islamic law), which forms the basis of Saudi law. [118] However, the judiciary is also largely subordinate to the executive branch, as judges are appointed by the king. [119] In addition, judges from the Specialized Criminal Court (SCC), which is routinely used to prosecute peaceful activists, have been subject to arbitrary arrest if their rulings fail to align with government preferences (see C3). [120]

A considerable increase in the length of prison sentences handed down by the SCC accompanied the appointment of judge Awadh al-Ahmari as the new president of the court in June 2022 (see C3). Previously, al-Ahmari was reported to have been part of a delegation sent by Saudi authorities to Istanbul in October 2018 to allegedly conceal evidence of the murder of journalist Jamal Khashoggi at the Saudi consulate. [121]

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

Laws designed to protect users from cybercrime contain clauses that limit freedom of expression. The 2007 Anti-Cyber Crime Law criminalizes "producing something that harms public order, religious values, public morals, the sanctity of private life, or authoring, sending, or storing it via an information network," and imposes penalties of up to five years' imprisonment and a fine of up to 3 million riyals ($800,000). [122]

Saudi authorities and state-run media outlets regularly remind citizens of the penalties applicable for breaching the Anti-Cyber Crime Law, the scope of which includes spreading rumors or "fabrications" on social media. [123] In March 2022, the government stated that those found guilty of spreading rumors pertaining to COVID-19 would face a potential five-year prison term and a fine of up to 1 million riyals ($270,000), warning that the fine would be doubled for repeat offenders. [124]

An antiterrorism law introduced in 2017 features broad definitions of terrorist acts. The legislation includes criminal penalties of five to 10 years' imprisonment for portraying the king or crown prince, directly or indirectly, "in a manner that brings religion or justice into disrepute," and a 15-year prison sentence for those using their "social status or media influence to promote terrorism." [125] International rights groups have condemned the antiterrorism law as unacceptably vague and inconsistent with international human rights standards. [126]

The SCC was initially founded in 2008 to try terrorism cases but has since been used to imprison human rights defenders and activists (see C3). [127]

C3 0-6 pts

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

Restrictive laws are rigorously applied to silence critical voices and human rights defenders—many of whom operate primarily online due to bans on traditional political organizing.

Authorities frequently arrest and prosecute activists and ordinary citizens for their social media content. In August 2023, Muhammad al-Ghamdi was sentenced to death by the SCC because of his X and YouTube activity. He was originally arrested in June 2022 and was convicted a year later of terrorism-related charges stemming from his commentary on social media, including his reposts of material from prominent government critics, though he had only 10 followers himself. [128] After the coverage period, the SCC overturned his death sentence; in September 2024, he was sentenced to 30 years imprisonment. [129] In May 2024, Muhammad's

brother, Asaad al-Ghamdi, was sentenced to 20 years in prison for social media posts that "harmed the security of the homeland." [130]

In January 2024, the SCC sentenced Manahel al-Otaibi, a fitness instructor and women's rights activist, to 11 years in prison at a secret hearing, having convicted her of terrorism offenses. Al-Otaibi was arrested in November 2022 and charged under the Anti-Cyber Crime Law for her social media posts in support of women's rights, and for posting photos of herself wearing "immodest" clothing. While in detention, she suffered physical abuse that resulted in a broken leg (see C7), as well as solitary confinement and enforced disappearance. [131]

Content creators have also faced arrest. In January 2024, Hatem al-Najjar, a journalist and podcast presenter, was arrested following a targeted hate campaign that called for his arrest, citing social media posts dating back to when he was a minor. [132] In July 2024, after the coverage period, the creator of the hit Netflix series *Masameer*, Abdulaziz al-Muzaini, was sentenced to 13 years in prison followed by a 30-year travel ban for allegedly "supporting terrorism and homosexuality" through content in the series, as well as social media posts dating back over a decade. In a now-deleted video, al-Muzaini announced his arrest and said he was ordered to shut down his production company and fire his staff. [133]

Others continue to serve long sentences for their online activity. Salma al-Shehab, a university student, received a 27-year prison sentence in early 2023, to be followed by a 27-year travel ban, merely for following activists and sharing their posts on X. [134] The charges for which al-Shehab was convicted include "assisting those who seek to cause public unrest and destabilize civil and national security" via social media. [135] Nourah bint Saeed al-Qahtani was sentenced in 2022 to 45 years in prison, the longest sentence for peaceful activism to date, after being charged with "using the internet to tear [Saudi Arabia's] social fabric." [136] Abdulrahman al-Sadhan, a 37-year-old former Red Crescent aid worker, remains imprisoned after receiving a 20-year sentence in 2021 for a satirical Twitter account that mocked conservative religious and government figures. Al-Sadhan's case was reportedly connected to the infiltration of Twitter in 2014 and 2015 by government agents who obtained jobs at the company (see C5). [137]

Authorities have in the past prosecuted high-profile individuals for their online dissent amid a widespread crackdown on intellectuals, academics, clerics, and

critics of the ruling family. These included Salman al-Awdah, Awad al-Qarni, and Ali al-Omari, all prominent clerics who have large online followings and were arrested in 2017; al-Awdah may have been targeted in response to a Twitter post in which he encouraged the resolution of a diplomatic dispute between Saudi Arabia and Qatar. [138] In 2019, Middle East Eye reported that the three clerics would be sentenced to death, [139] though after years of delays in their court proceedings, [140] none had been executed at the end of the coverage period. In January 2023, it was reported that prosecutors had requested the death penalty for al-Qarni, who was charged with using Twitter, WhatsApp, and other social media platforms to share "hostile" information about the government (see B8). [141]

C4 0-4 pts

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

Encrypted communications are banned in Saudi Arabia, though this is not effectively enforced. [142] Authorities frequently attempt to identify and detain anonymous or pseudonymous users and writers who make critical or controversial remarks. Individuals are required to use their legal names when signing mobile-service contracts and must provide a national identification card or residence permit. [143] They also must have their fingerprints processed. [144] This information is then saved in a database maintained by the Interior Ministry. In January 2016, the CST required mobile service providers to register the fingerprints of new SIM-card subscribers within 90 days, or those users would face permanent suspension. [145]

It is common for Saudi social media users to employ pseudonyms or communicate via anonymous channels or applications, such as the anonymous messaging app Jodel. However, some individuals who posted anonymously have nonetheless been identified and prosecuted. [146]

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**0** / 6

Surveillance is rampant in Saudi Arabia, and the authorities increasingly rely on advanced spyware to monitor Saudi journalists and internet users, both domestically and abroad. [147]

Saudi authorities regularly monitor websites, blogs, chat rooms, social media sites, emails, and text messages. The government justifies the pervasive surveillance of nonviolent political, social, and religious activists by claiming that it is protecting national security and maintaining social order. After the government announced that it would lift its ban on online voice and video call services in 2017, it claimed that all calls would be monitored and censored by the CST. [148] Saudi surveillance activities prompted the European Parliament to approve a resolution calling for an embargo on sales of surveillance equipment to the country in 2018. [149]

The government has continued to invest in sophisticated spyware and digital surveillance systems. According to Citizen Lab, a Canadian watchdog organization, spyware developed and sold by the Israeli firm NSO Group has been used to target activists and dissidents in Saudi Arabia. In December 2021, Citizen Lab reported that the Saudi authorities had likely begun using Predator spyware, distributed by the North Macedonia–based company Cytrox. [150] A report by Meta also stated that Saudi entities were likely among Cytrox's customers. [151] In February 2024, Saudi's Public Investment Fund (PIF) announced a $200 million partnership deal with Dahua Technology, a major Chinese surveillance technology company. [152]

Even members of the royal family have been targeted for surveillance. In August 2022, Abdullah bin Faisal al-Saud, a minor member of the family, was sentenced to 30 years in prison due in part to phone calls he had made over Signal, during which he discussed a family member who had previously been imprisoned in Saudi Arabia. [153] It is unclear what specific methods were used by the government to monitor his private conversations. [154]

In February 2022, Reuters reported that an "unusual error" in NSO's spyware—discovered on Saudi activist Loujain al-Hathloul's smartphone—provided direct evidence that the company had built an espionage tool that penetrates devices without interaction from the user. [155] Al-Hathloul had been targeted with NSO spyware in the past on behalf of the Saudi government, as have other Saudi activists like Omar Abdulaziz. [156] A lawsuit has been filed in a US District Court

against DarkMatter, an Emirati spyware company, and three of its former senior US executives for their role in the hacking of al-Hathloul's devices in 2017. While living in the UAE in 2018, al-Hathloul had been hacked, arrested by the country's security services, and forcibly deported back to Saudi Arabia, where she was imprisoned. [157]

In October 2021, reports emerged that *New York Times* journalist Ben Hubbard had been subjected to several phone hacking attempts, likely by Saudi authorities. [158] Research by Citizen Lab found that he was targeted with Pegasus spyware between June 2018 and June 2021 while he was reporting on Saudi Arabia and writing a book on Crown Prince Mohammed bin Salman. [159]

According to a report by the *New York Times* in July 2021, Israeli authorities "secretly authorized" and encouraged at least four Israeli cybersurveillance companies to work for the Saudi government, including Verint, Candiru, and Quadream. [160] The Israeli firm Cellebrite has also provided phone-hacking services to the Saudi government. [161]

Saudi Arabia has a record of recruiting agents to infiltrate technology platforms and online resources. In a May 2023 civil suit in the United States, X was accused of disclosing confidential user data to Saudi authorities and facilitating human rights abuses against dissidents. [162] In December 2022, a US court in California found that Ahmad Abouammo, a Saudi national and former Twitter employee, had taken bribes from the Saudi government in exchange for sharing the private data of Saudi dissident Twitter users. [163] In the same month, Wikimedia banned 16 Wikipedia content editors, some of whom were reportedly Saudi nationals, following an internal investigation that implicated them in "conflict-of-interest editing" and coordination with "external parties." The content editors had primarily edited content relating to Saudi Arabia (see B5 and C3). [164]

C6 0-6 pts

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

Given Saudi Arabia's highly restrictive regime and known surveillance efforts, telecommunications companies likely retain and intercept customer data for use by law enforcement agencies and state authorities.

In September 2021, the government published the Personal Data Protection Law (PDPL), which regulates the collection, processing, storing, and transfer of data. The law contains many safeguards typical of robust data-protection laws around the world, including a user-consent requirement for disclosure of most information, and penalties for unauthorized transfers of data. However, these safeguards are undermined by other provisions that allow the government to access collected data. [165] According to the law, the Saudi Data and Artificial Intelligence Authority (SDAIA), a government agency, would be the industry regulator for at least two years. In November 2022, the SDAIA published an amended version of the PDPL that included business-friendly changes, such as a relaxation of strict data-localization conditions. [166] The amended law came into effect in September 2023. [167]

In March 2020, the *Guardian* reported on data revealed by a whistleblower that allegedly showed millions of secret location-tracking requests originating via STC, Mobily, and Zain between November 2019 and February 2020. According to experts, the efforts to establish the US location of Saudi-registered mobile phones suggested a systematic spying campaign orchestrated by the Saudi government, though it was unclear whether the mobile service providers were knowingly complicit. [168]

In January 2024, the CST approved the Regulations for Providing Digital Content Platform Services, a proposed regulatory framework for digital content platforms that included requirements for local and foreign companies to apply for licensing through CST, comply with all CST requests, and imposed additional fees on providers (see B2 and B6). Digital service providers have until October 2024 to comply with the regulation. [169]

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

The government reportedly maintains a secret campaign to monitor, detain, kidnap, and torture dissidents. While these practices existed before Crown Prince Mohammed bin Salman came to power, they have worsened under his rule. [170] Many individuals detained for their online activism have reported physical abuse

including torture while in custody, [171] and deaths have also been reported. [172] The government persecutes dissidents' relatives, and dissidents have faced threats and violence even after fleeing Saudi Arabia.

Those detained and imprisoned for their online activities have reportedly experienced torture in custody (see C3). [173] Manahel al-Otaibi, who is serving an 11-year prison sentence for her social media activity, was subject to physical abuse in detention, resulting in a broken leg. [174] Abdulah Jelan, who is currently serving a 10-year prison sentence over social media posts about unemployment in Saudi Arabia, has been subjected to torture, ill-treatment, and denial of medical care. [175] Members of the Huwaitat tribe of northwestern Saudi Arabia who published videos online to protest their forced eviction have been tortured in custody. One member, Shadli al-Huwaiti, reportedly went on hunger strike to protest his ill-treatment in prison. [176] Abdulrahman al-Sadhan, who is serving a 20-year prison sentence over a satirical Twitter account, has reportedly been subjected to severe torture and prolonged periods of solitary confinement. [177]

In July 2021, Human Rights Watch (HRW) published reports in which an individual identifying himself as a Saudi prison guard detailed "brutal torture" of high-profile political detainees at a prison in Dhahban as well as at another "secret prison." According to HRW, Saudi authorities failed to independently investigate allegations of torture, which included descriptions of electric shocks, whippings, and sexual assault. [178]

Forcible disappearances of online activists, journalists, or government critics have occurred in the past. Turki al-Jasser, a Saudi writer who was arrested in 2018 and forcibly disappeared in the Saudi prison system after running a Twitter account that was critical of the government, has reportedly been subjected to severe torture. [179] His whereabouts and condition remained unknown during the coverage period, with earlier rumors suggesting that he had died under torture. [180]

In February 2021, the *Washington Post* reported on the disappearance of Ahmed Abdullah al-Harbi, a Canada-based Saudi dissident who visited the Saudi embassy in Ottawa that January and later reappeared in Saudi Arabia. Al-Harbi's fellow activists claimed that his return was coerced by Saudi authorities, citing fears that he had been pressured to reveal identifying information that would endanger the

activists and their families. [181] Al-Harbi's whereabouts remained unknown at the end of the coverage period.

Private actors have been encouraged by authorities to harass government critics online. [182] Former royal adviser Saud al-Qahtani, who reportedly managed the so-called electronic army before being sidelined in the wake of Jamal Khashoggi's 2018 murder (see B5), was known for overseeing online campaigns that harassed bloggers and activists, and he reportedly kept a blacklist of government enemies, urging citizens to add the names of those allegedly engaging in treachery or showing a lack of patriotism. [183] Subsequent evidence suggests that citizens have adopted similar tactics, contributing to a climate of fear. [184]

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

While activists and government critics have experienced cyberattacks in the past, such as the surreptitious installation of spyware on their phones, fewer cases were reported during this report's coverage period, and more generally over recent years. Given the rise in government-led censorship and the increasing limits on freedom of expression, authorities may depend less on technical attacks to silence independent journalists or human rights activists and organizations.

In October 2022, the digital risk management company CloudSEK found that several phishing domains targeting and impersonating Absher, the Saudi government's service portal, were giving fake services to citizens while stealing their credentials. [185]

Several public and private institutions and projects have faced security breaches in recent years. In July 2021, 1,000 GB of data from the Saudi national oil company, Saudi Aramco, was seized by unknown extortionists on a dark webpage, who offered to delete the stolen data in exchange for $50 million in cryptocurrency. In May 2020, Chafer, a hacking group with apparent links to Iran, was found to have targeted Saudi air-transport and government entities as far back as 2018. [186]

The Saudi government has reportedly been tied to attacks on foreign news outlets and journalists. In June 2019, the *Guardian* was warned that a Saudi "cybersecurity unit" had targeted it with the aim of hacking into the email accounts of journalists who were investigating the royal court (see C5). [187] In December 2020, Al-Jazeera journalist Ghada Oueiss was subjected to a hacking operation allegedly led by Saudi and Emirati officials (see C5). [188]

Footnotes

1 Simon Kemp, "Digital 2024: Saudi Arabia," DataReportal, February 23, 2024, https://datareportal.com/reports/digital-2024-saudi-arabia

2 Simon Kemp, "Digital 2024: Saudi Arabia," DataReportal, February 23, 2024, https://datareportal.com/reports/digital-2024-saudi-arabia

3 "MCIT Annual Report 2023," MCIT, 2023, https://www.mcit.gov.sa/sites/default/files/2024-04/MCIT_Annual%20Repor...

4 Ian Fogg, "Benchmarking the Global 5G Experience — June 2023", June 30, 2023, https://www.opensignal.com/2023/06/30/benchmarking-the-global-5g-experi...

5 "FACT SHEET: Results of Bilateral Meeting Between the United States and the Kingdom of Saudi Arabia," July 15, 2022, The White House, https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/15...

More footnotes

On Saudi Arabia

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

See More ›

Country Facts

Population
36,410,000

Global Freedom Score
9 /100 **Not Free**

Internet Freedom Score
25 /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 2024

Other Years

2025

ADDRESS

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

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org