

— [Our Issues](#) [Countries](#) [Policy Recommendations](#) [Explore the Map](#)

## FREEDOM ON THE NET 2020

# United Arab Emirates

**29**  
/100

NOT FREE

A. <u>Obstacles to Access</u>	<b>12</b> /25
B. <u>Limits on Content</u>	<b>10</b> /35
C. <u>Violations of User Rights</u>	<b>7</b> /40

### LAST YEAR'S SCORE & STATUS

**28** /100 **Not Free**

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

## Overview

Internet freedom in the United Arab Emirates (UAE) improved slightly this year, although the overall environment remains significantly restricted. Fewer citizens, online activists, and journalists received long prison sentences for content posted online, however a number of people were arrested for their social media posts. Online censorship is rampant and government surveillance is still problematic.

The UAE is a federation of seven emirates led in practice by



### On United Arab Emirates

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

Abu Dhabi, the largest by area and the richest in natural resources. Limited elections are held for a federal advisory body, but political parties are banned, and all executive, legislative, and judicial authority ultimately rests with the seven hereditary rulers. The civil liberties of both citizens and noncitizens—the latter of which make up an overwhelming majority of the population—are subject to significant restrictions.

[See More >](#)

## Key Developments, June 1, 2019 - May 31, 2020

- In September 2019, UAE internet service provider (ISP) Etisalat announced that the Asia-Africa-Europe-1 (AAE-1) undersea cable had come online. It is the largest global submarine cable system in the world and connects Europe and East Asia (see A1).
- While many popular Voice over Internet Protocol (VoIP) services remained blocked, some platforms such as Skype for Business and Zoom became available as more people were forced to work from home during the COVID-19 pandemic (see A3).
- Pro-government commentators continued to spread propaganda during the coverage period. Specifically Twitter removed 9,000 pro-UAE accounts that were spreading propaganda about the coronavirus (see B5).
- During the COVID-19 pandemic, the government issued a fine of up to 20,000 dirhams (more than \$5,400) if people share medical information (including online) about the coronavirus that contradicts official statements (see C1).

### Country Facts

Global Freedom Score

**17/100**

**Not Free**

Internet Freedom Score

**29/100**

**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 2020

# A. Obstacles to Access

Other Years

2019

*Emirati internet users enjoy a robust information and communications technology (ICT) infrastructure and high connection speeds. However, the major telecommunications companies are either fully or partially state-owned, resulting in high prices and weak competition. Popular VoIP services are subject to blocking, however during the COVID-19 pandemic some messaging platforms became available.*

**A1** 0-6 pts

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

**6/6**

The UAE is one of the world's most connected countries. According to the International Telecommunication Union (ITU), 98.5 percent of the population used the internet in 2018, up from 94.8 percent the previous year. **1** As of December 2019, there were nearly 3.04 million internet subscribers in the country, 100 percent of whom had broadband connections. **2** The UAE has one of the highest mobile phone penetration rates in the region; the ITU reported 208.5 mobile subscriptions per 100 inhabitants in 2018. **3**

In May 2019, the mobile service provider Etisalat became the first in the Middle East and North Africa region to launch fifth-generation (5G) services. The operator has partnered with Chinese smartphone manufacturer ZTE to offer the service. **4** A month later, the company Du launched their 5G service, also through a partnership with ZTE. **5** Moreover, Etisalat has increased its broadband speeds, offering up to 1 Gbps for certain home plans and speeds of up to 600 Mbps—up from 100 Mbps—for several business

services. **6**

Damage to undersea cables occasionally disrupts connectivity, **7** though no incidents were reported during the coverage period. In December 2018, various telecommunications companies, including Etisalat, signed an agreement to create a new submarine cable system by 2021 linking South Africa, the Middle East, Pakistan, and Europe. One of the stations will be based in the emirate of Fujairah.

**8** In September 2019, Etisalat announced that the Asia-Africa-Europe-1 (AAE-1) undersea cable had come online. It is the largest global submarine cable system in the world and connects Europe and East Asia. It was launched in partnership with Etisalat and 18 other global telecommunications companies. According to Etisalat, the AAE-1 “will allow Etisalat to diversify its sources of data and increase speeds it can offer business and general public customers—while also reducing stress on its existing network caused by ever-exploding volumes of data being transmitted.” **9**

In October 2018, *Gulf Business* reported that 10,800 taxis in Dubai would offer free Wi-Fi as part of a phased project that began with 500 Dubai airport taxis in 2016. **10** Authorities and local press continue to warn against using free public Wi-Fi networks due to privacy concerns. **11** In light of the 2020 COVID-19 lockdown, the Telecommunications Regulatory Authority (TRA) announced in March 2020 that any homes without internet will be provided free internet data via mobile phones to help increase access to distant learning platforms for students. **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**

**1/3**

reasons?	
----------	--

While prices are among the highest in the region, broadband is affordable for most users given the country's high per capita income. **13** In May 2019, a survey found Dubai to be the most expensive city in the world for broadband costs. **14** A November 2018 survey by the UK telecommunications company Cable found that the average cost of broadband in the UAE is \$10.23 for 1 GB, nearly 20 percent more than the global average of \$8.53. **15** In July 2019, the TRA required Etisalat and Du to discontinue their pay-per-use data plans "in order to protect the subscribers from excessive charges." **16**

An Etisalat post-paid mobile plan with a 6 GB data allowance and 500 local minutes **17** costs 150 dirhams (\$40), while a prepaid plan with an allowance of 3.5 GB and 175 minutes costs 130 dirhams (\$35). **18** In 2017, the telecommunications regulator directed mobile service providers to reduce rates for UAE residents roaming within the Gulf region, resulting in an average 18 percent drop in prices for consumers. **19** Later that year, Etisalat announced a 5 percent value-added tax (VAT) on all products and services beginning in January 2018. **20** In March 2019, based on input from consumers, the Telecommunications Regulatory Authority (TRA) lowered the cost of cancelling a mobile contract to one month's rental fee; the previous cost was one month multiplied by the number of months left over. **21** The policy went into effect in January 2020. **22**

Emirati schools are increasingly connected to the internet and equipped with e-learning facilities, and many offer tablets for student use. **23** There are also programs for principals to enroll in international computer-literacy training programs. **24** In October 2018, the government launched Madrasa, a free digital platform estimated to

provide 50 million primary and secondary school students in the region with 5,000 instructional videos, all translated into Arabic, on topics including science and mathematics. **25**

### A3 0-6 pts

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

No orders to shut down ICT networks were reported during the coverage period, but authorities restrict a number of communication platforms.

Most popular VoIP services are restricted over mobile connections. Etisalat and Du are the only companies licensed to provide paid VoIP services, while the free or low-cost over-the-top (OTT) voice call services provided by WhatsApp, Skype, and others are only accessible through fixed-line or Wi-Fi connections. In March 2020, the TRA allowed the use of Skype for Business, Google Hangouts, Blackboard, Microsoft Teams, and Zoom “to support distance learning and working from home,” stressing that this change comes “exceptionally until further notice.” **26**

In August 2018, users reported that Du had unblocked the voice chat function within various online video games. **27** WhatsApp’s voice feature was blocked shortly after it was introduced in 2015, **28** as was a similar feature offered by Facebook. **29** Viber has been banned since 2013, along with FaceTime, Apple’s video chat product. **30** Apple agreed to sell its iPhone products to UAE mobile phone companies without the FaceTime app preinstalled, though it can be used on phones purchased outside the country. **31** The VoIP feature for Discord, a chatting app used by gamers, was blocked in 2016. **32**

Seeking to improve connectivity within the country, Etisalat and Du have launched their own carrier-neutral international internet exchange points (IXPs), called SmartHub and Datamena, respectively. **33** Etisalat maintains its nationwide fiber-optic backbone. In 2015, the company selected TeliaSonera International Carrier (TSIC) as its preferred global internet backbone provider. **34**

**A4** 0-6 pts

<p><b>Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?</b></p>	<p><b>2/6</b></p>
--	-------------------

Internet service providers (ISPs) in the UAE are either fully or partially owned by the state, allowing authorities to exert control over the flow of information. The country's two largest mobile service providers, Etisalat and Du, are both controlled by the state. The government maintains a 60 percent stake in Etisalat through its ownership in the Emirates Investment Company, **35** while a majority of Du is owned by various state companies. **36** Du pays a percentage of its profits and revenue as a dividend to the government, which owns 39.5 percent of the company through its sovereign wealth fund, the Emirates Investment Authority.

**37** In 2015, the government announced a decision to allow up to 20 percent of Etisalat shares to be held by foreign investors. **38**

In 2017, the Emirates Integrated Telecommunications Company (EITC), one of the companies that owns Du, launched a new mobile service provider under the Virgin Mobile brand. Due to the EITC's ownership of Du, the new provider was not required to obtain a separate license. **39**

In April 2018, Etisalat announced "the first global cybersecurity alliance" with Singapore's Singtel, Japan's

Softbank, and Spanish blue-chip firm Telefonica, **40** which will reach over one billion consumers in 60 countries. The alliance will pool together network intelligence on threats to cybersecurity, in addition to combining resources to serve customers. **41** In September 2019, Etisalat Group announced that it had acquired full ownership of Help AG's businesses in the UAE and Saudi Arabia, a cybersecurity company in the Middle East and North Africa. Etisalat said that the acquisition will allow them to "diversify the digital portfolio and will accelerate the growth of Etisalat's existing cyber security activities." **42**

**A5** 0-4 pts

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

Regulatory bodies frequently fail to operate in a free and fair manner. The TRA oversees service providers and makes executive decisions regarding monitoring, filtering, and banning services and websites, without any oversight or transparency. Providers must follow the laws and regulations set by the TRA, which was established in 2003 to manage "every aspect of the telecommunications and information technology industries in the UAE." Its objectives include ensuring quality of service and adherence to terms of licenses by licensees, encouraging telecommunications and information technology (IT) services within the UAE, resolving disputes between the licensed service providers, establishing and implementing a regulatory and policy framework, and promoting new technologies. **43**

The TRA's current chairperson is Major General Talal Hamid Belhoul, who was also appointed director general of the State Security Department in Dubai in 2017. **44** The current

director of the TRA, Hamad al-Mansoori, was appointed in 2015. Among the many government positions he has held, al-Mansoori is also the chairperson of the Mohammed Bin Rashid Space Center and the vice chairman of the Emirates Space Agency. **45**

## B. Limits on Content

*Authorities continued to block a number of websites containing criticism of the government and other sensitive content. In recent years, the repressive environment, marked by the threat of legal action or harassment, and high levels of surveillance have led to increased self-censorship. Twitter removed 9,000 pro-UAE accounts that were spreading propaganda about the coronavirus.*

**B1** 0-6 pts

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

**1/6**

While ISPs are required by the TRA to block content related to terrorism, pornography, gambling, and political speech threatening to the ruling order (see B3), in practice authorities also commonly block websites that criticize the government or tackle social taboos. Blocking has emerged as a political tool through which authorities sought to isolate Qatar, which Bahrain, Egypt, Saudi Arabia, and the UAE had accused of supporting “terrorist” groups, notably the banned Muslim Brotherhood. In 2017, authorities blocked a number of Qatari media sites amid this dispute, including Al Jazeera Live. **46**

The TRA reported that it had blocked 1,688 websites in 2019; 32 percent of which for pornography, 25 percent for fraud and phishing, and 15 percent for bypassing blocked content.

The report also mentions that one unnamed website was blocked upon judicial order. The TRA blocked 38 websites during 2019 categorized under “offenses against the UAE and public order.” **47**

In October 2018, the TRA reported that it had blocked 1,666 websites in the first half of the year, compared to 2,256 during the same period in 2017. Using automatic filtering systems, 47.6 percent of the websites were blocked for pornographic content, 28 percent for scams and fraud, and the rest for drugs, piracy, terrorism, and other “illegal activities.” **48** In March 2019, the government blocked the newly established news site Al-Estiklal, which is critical of a number of regimes in the region. As of June 2020 it is still blocked. **49** In April 2019, a blogger reported that the citizen media platform Global Voices was apparently blocked by Etisalat. **50** As of June 2020, the website appears to no longer be blocked on either provider.

Many other sites critical of the government have been blocked, including the UK-based, English-language news site Middle East Eye, which was blocked in 2015 after it published articles exposing the country’s harsh surveillance practices and poor human rights record. **51** The New Arab, which is based in the United Kingdom and funded by a Qatari businessman, was blocked in 2015 without explanation. **52** Also in 2015, authorities blocked Arabic-language sites run by news agencies in Iran, such as Al-Alam TV, over allegations that they disseminated anti-government propaganda. **53**

The Beirut-based Gulf Center for Human Rights is blocked, **54** as is the LGBT+ sports news site Outsports. **55** In July 2018, Canadian digital rights organization Citizen Lab reported that the website of the International Lesbian, Gay, Bisexual, Trans, and Intersex Association was blocked in the

UAE, using internet filtering technology produced by the Canadian company Netsweeper. **56**

As of June 2020, several political blogs, **57** a number of atheist and secular websites, **58** at least one site disseminating news on Emirati political detainees and prison conditions, **59** and sites related to the Muslim Brotherhood and regional nongovernmental organizations (NGOs) are blocked. **60** The website of the Islamic Human Rights Commission (IHRC) was also blocked. **61** Users have reported the blocking of social media content relating to political detainees in the past, **62** as well as Archive.today, a tool that retains URLs that might be removed from the internet or be modified. **63**

Citizens use social media platforms to report blocked content and platforms, sometimes addressing their questions to the two main service providers. During the coverage period, users on Twitter reported that the streaming service Spotify has been blocked by Du **64**, as well as the subscription-based content service OnlyFans **65** and the VoIP service TeamSpeak. **66** In response to an online inquiry, Du confirmed that TeamSpeak is blocked as are all VoIP services. **67**

According to a 2013 Citizen Lab Report, ISPs use advanced tools such as SmartFilter, Netsweeper, and Blue Coat ProxySG to censor content. **68** The organization has also documented websites that are blocked in the UAE because both SmartFilter (used by Etisalat) and NetSweeper (used by Du) have miscategorized them as pornographic. **69** Citizen Lab again confirmed the use of NetSweeper in an April 2018 report. **70**

**B2** 0-4 pts

**Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?**

**1/4**

The TRA has also been able to censor selected content on platforms such as YouTube, Facebook, and Twitter, according to local users. Facebook occasionally receives government requests to remove content. In 2019, Facebook reported that it received 11 requests from the UAE: 1 for a page, and 10 for posts. Facebook explains in their transparency report: “We restricted access in the UAE to 10 items containing allegations of the UAE’s interference in Algeria’s internal affairs that were reported by the Telecommunications Regulatory Authority. We also restricted access to one item in response to a private report of defamation.” **71**

In 2019, Google reported receiving 50 removal requests from the UAE regarding copyright—as opposed to 3 requests in the first half of 2018—most of which fell under “trademark” issues. **72** Twitter reported 112 removal requests from the UAE government from July to December 2018, of which it complied with none. **73**

Late in 2019, the video-chat ToTok app became popular in the country and later around the world. The app was not blocked by local VoIP rules, and later was found out to be an Emirati app meant to spy on all conversations and messages among users, prompting its removal from Apple and Google stores (see C5). **74**

**B3** 0-4 pts

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

**2/4**

process?	
----------	--

Some restrictions on digital content lack proportionality and fairness. The TRA instructs ISPs to block content related to terrorism, pornography, gambling, and political speech considered threatening to the ruling order.

Using banned VoIP services through a virtual private network (VPN) is punishable under a law that bars the use of VPNs to commit a crime, as well as cybercrime and telecommunications regulatory laws. **75** Convictions under cybercrime laws can lead to a fine of between 500,000 (\$136,000) and 2 million dirhams (\$544,000), jail time, or both. **76**

Du details the criteria it uses to block sites in a document available on its website. Prohibited content includes information related to circumvention tools, the promotion of criminal activities, the sale or promotion of illegal drugs, dating networks, pornography, LGBT+ content, gambling sites, unlicensed VoIP services, terrorist content, and material that is offensive to religion. **77** No similar list has been made available by Etisalat, although the company invites users to request the blocking or unblocking of sites.

**78** Du also allows users to send unblocking requests to a designated email address and blocking requests through an online form. **79** However, neither company provides information on whether sites have been unblocked as a result of requests. **80** Twitter users sometimes monitor when sites are blocked to combat the lack of transparency, **81** but the TRA has also called on social media users to help report “suspicious” content for blocking.

Online content is often removed without transparency or judicial oversight. Under the cybercrime law, intermediaries, such as domain hosts or administrators, are liable if their

websites are used to “prompt riot, hatred, racism, sectarianism, or damage the national unity or social peace or prejudice the public order and public morals.” **82**

Website owners and employees may also be held liable for defamatory material appearing on their sites. **83**

Regulations instituted in October 2018 require social media influencers to identify content defined as advertisements (see B6) and allow the National Media Council to remove content that violates the guidelines. **84**

**B4** 0-4 pts

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

Self-censorship online has worsened in recent years, due to the risks of legal action or harassment in retaliation for online activities, as well as high levels of surveillance.

Virtually nobody within the country speaks out on political and other sensitive issues. **85** Local news sites, many of which are owned by the state, exercise self-censorship in accordance with government regulations and unofficial red lines. Overall press freedom is poor, and foreign journalists and scholars are often denied entry or deported for expressing their views on political topics, further chilling the environment for online expression. **86**

The United Arab Emirates has an advanced surveillance system, which includes all online modes as well as real life monitoring of public spaces. Media outlets in the country are either owned by the state or must abide by its image and rules in order to operate. The constitution emphasizes that freedom of expression is limited. Cases of blocking content as well as persecuting journalists are rarely handled with transparency. The judiciary system plays no role in balancing powers and protecting users’ rights. With the cybercrime

law and latest regulations for social media, there is no room for expression that can go without state persecution, leading users to self-censor their online content.

**B5** 0-4 pts

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

The government has allegedly manipulated the online information landscape to advance its interests. In 2014, the government spent more than \$12 million on public relations firms, which some observers suspect had been deployed to counter allegations of human rights abuses online. **87** A large number of anonymously operated Twitter accounts appear dedicated to harassing and intimidating political dissidents and their families online.

In September 2019, Twitter announced that it took down approximately 4,525 accounts linked to Saudi Arabia, the United Arab Emirates, and Egypt. It was found that 4,248 of these accounts were operating from the UAE. Twitter accused all of the accounts of promoting “political spam.”

**88** In April 2020, Twitter took down a pro–United Arab Emirates network of roughly 9,000 accounts that spread propaganda about the coronavirus pandemic and criticized Turkey’s military intervention in Libya. The network had been tied to marketing firms in the region, and parts of this network had already been removed by Facebook and Twitter in 2019. **89**

In an article published in July 2019 by Al Jazeera, experts pointed to thousands of bot accounts attempting to influence views on the Qatar blockade crisis by spreading fake news, retweeting officials, and amplifying hashtags.

While the source of these accounts is unclear, according to the report, “prominent Twitter influencers in Saudi and the UAE later tweeted about the bot-created subject, that was then picked up by ‘real people.’” <sup>90</sup>

**B6** 0-3 pts

<p><b>Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?</b></p>	<p><b>1/3</b></p>
---	-------------------

Authorities impose economic and regulatory constraints that limit the ability of anti-government websites to produce content online. For example, the government reportedly pressured the Dubai-based advertising agency Echo to end its advertising contract with the US-based news outlet *Watan*. <sup>91</sup>

In March 2018, the state media oversight body, the National Media Council, announced new regulations for electronic media that would govern “all online activities, including e-commerce; publishing and selling of print, video, and audio material; as well as advertising.” <sup>92</sup>

Social media influencers who engage in commercial activities or promote products must now apply for licenses, which are awarded based on a number of qualifications, such as age, a clean criminal record, good reputation, and a university degree. <sup>93</sup> The regulations went into effect at the beginning of the reporting period. <sup>94</sup> In June 2019, It was reported that more than a thousand people had been granted licenses to operate as social media influencers in the UAE since the new regulation came in place. <sup>95</sup> The National Media council warned social media influencers of a 5,000 dirham (\$1,361) fine for not obtaining licenses. An official stated they “have a team dedicated to monitoring illegal activities on social media and other online platforms.”

**96**

In October 2018, the council issued 19 rules for advertising, stating that “advertisements must be identified on social media clearly.” The rules also include “showing respect for the UAE’s systems and policies at an internal level and its relations with other countries, avoiding images that harm public morality, respecting intellectual property rights and a ban on tobacco advertising of any kind.” Violators could be subject to a 5,000 dirhams (\$1,360) fine, with additional fees if the fine is not paid within five days. Repeat violations could lead to fines of up to 20,000 dirhams (more than \$5,400).

**97****B7** 0-4 pts

<b>Does the online information landscape lack diversity?</b>	<b>1/4</b>
--	------------

The blocking of anti-government and other sensitive content (see B1) and the criminalization of VPNs limit the diversity of the online information landscape. Moreover, many local news sites self-censor, further reducing the diversity of viewpoints online (see B4). However, according to Northwestern University in Qatar’s 2018 Media Use in the Middle East survey, 71 percent of UAE nationals accessed news online. **98**

**B8** 0-6 pts

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

Some Emiratis push back against government repression through online activism, but the repressive legal and regulatory environment limits their effectiveness. In the

past, families of political prisoners frequently relied on Twitter to speak on behalf of detainees, document allegations of torture, and call for their release. However, the practice has become less frequent in recent years due to escalating arrests and prosecutions. With widespread arrests, intimidation, surveillance, and retaliation that users face for speaking out online, the only voices critical of the regime today are based abroad.

In response to the 2017 blocking of Skype, a user initiated an online petition to unblock it, which received thousands of signatures. The TRA responded by blocking Change.org, the platform on which the petition was posted. <sup>99</sup> Laws prohibit calling for, promoting, and collecting donations online without obtaining prior permission and licensing from authorities. <sup>100</sup>

## C. Violations of User Rights

*While fewer people received long prison sentences, users were still arrested for their online content. Prominent activist Ahmed Mansour went on a hunger strike during his 10-year prison sentence to protest torture and terrible prison conditions. Surveillance activities are conducted with little judicial oversight. During the coronavirus pandemic, the government issued a law penalizing the spreading of false information.*

**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**

Article 30 of the constitution states that freedom of opinion “shall be guaranteed within the limits of law.” However, many laws can effectively limit free speech online, and these rights are not respected in practice. **101** Moreover, the judicial system is not independent, as there is significant executive influence. **102** Under a 1980 law, authorities can “censor local or foreign publications if they criticize domestic policies, the economy, the ruling families, religion, or the UAE’s relations with its allies.” **103**

The judiciary enjoys no independence in the UAE. Judicial bodies, judges, as well as lawyers have no public profiles, especially not in criticism of the state. The only lawyer to represent political detainees, Mohammed al-Roken, continues to serve a prison sentence for his work. **104** Smear campaigns against dissidents go without investigation. Online journalists and bloggers are not allowed anonymity, and are required to register for permits, as per the social media law. With the cybercrime law and hate crimes law, the regime has stifled freedom of expression in the country.

During the COVID-19 pandemic, in April 2020, the government issued a fine of up to 20,000 dirhams (more than \$5,400) if people share medical information about the coronavirus that contradicts official statements; including sharing this information online. **105**

**C2** 0-4 pts

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

**0/4**

There are a number of laws that assign criminal penalties for online activities. Since a series of regional mass uprisings in 2011, the UAE has followed countries of the Gulf

Cooperation Council (GCC) in passing legislation to criminalize criticism of authorities online. **106**

The cybercrime law criminalizes a wide range of legitimate online activities. Hefty fines and jail sentences can be handed down for gambling online, disseminating pornographic material, or sharing content that is perceived to violate another person's privacy. **107** The cybercrime law also criminalizes offending the state and its rulers or symbols, and insulting religion. Calls to change the system of government are punishable by life imprisonment. Authorities have repeatedly warned foreign nationals that they must also follow the country's restrictive laws. **108** In 2017, the government expanded the cybercrime law to criminalize "sympathy for Qatar," which can be punished with a 15-year prison sentence and a fine. **109**

In August 2018, the president amended three articles in the cybercrime law. Changes to Article 26 stipulate harsher penalties for enabling communication between terrorist groups or any other "unauthorized group." The broadly worded article provides for 10 to 25 years of imprisonment and a fine between 2 million (\$544,000) and 4 million dirhams (\$1.1 million). It also prescribes up to five years in prison and a fine between 500,000 (US\$136,000) and 1 million dirhams (\$272,000) for inciting hatred. The other two amendments are related to incitement, endangering national security and state interests (Article 28), and deporting foreigners (Article 42). **110** In June 2019, the TRA announced that cybercrime laws and regulations "will soon be enhanced to combat the ever-growing threat of cybercrimes," as part of the new National Cybersecurity Strategy that will be implemented across nine sectors. **111**

In January 2019, an official from the Interior Ministry listed ten types of social media activities considered illegal under

the cybercrime law: defaming or disrespecting others, violating privacy, filming people or places and posting these videos without permission, spreading fake news and rumors, manipulating personal information, blackmail and threats, establishing websites or accounts that violate local regulations, inciting immoral acts, posting work-related confidential information, and establishing or managing websites or accounts to coordinate with terrorist groups.

**112**

Broadly worded provisions of a 2015 hate speech law, which criminalize insults to “God, his prophets or apostles or holy books or houses of worship or graveyards,” open individuals up to criminal charges for expressing nonviolent opinions on religion. Penalties under the law range from prison terms between six months and 10 years and fines between 50,000 (\$13,600) and 2 million dirhams (\$544,000). **113**

Furthermore, while the law bans discrimination on the basis of “religion, caste, doctrine, race, color, or ethnic origin,” it does not protect those persecuted on the basis of gender or sexuality. **114** The law specifically covers online as well as offline speech.

Terrorism offenses are punishable by life imprisonment, death, and fines of up to 100 million dirhams (\$27.2 million).

**115** Under the law, citizens may be charged with such broad crimes as undermining national unity, possessing materials counter to the state’s notion of Islam, and “publicly declaring one’s animosity or lack of allegiance to the state or the regime.” **116**

Articles 8 and 176 of the penal code are used to punish public “insults” against the country’s top officials and calls for political reform. **117** Articles 70 and 71 of a 1980 publishing law prohibit criticism of the head of state, Islam, or any other religion. **118** In 2016, Dubai police reiterated

that posting pictures of others without permission can lead to six months in jail and a fine between 150,000 (\$41,000) and 500,000 dirhams (\$136,000). **119**

**C3** 0-6 pts

**Are individuals penalized for online activities?**

**2/6**

*Score Change: The score improved from 1 to 2 due to fewer long convictions reported during the coverage period, although people continue to be arrested for content they post online.*

The government routinely jails individuals for posting political, social, or religious opinions online, and long prison sentences have been handed out on such charges in recent years. Online activists face arbitrary detention. Arrests for online activity continued throughout the reporting period. However, no long prison sentences were reported during the coverage period.

In December 2018, a court rejected activist Ahmed Mansour's final appeal on a 10-year prison sentence and 1 million dirhams (US\$272,000) fine. Reports also suggested that he would be subject to three years of surveillance after his release. **120** He was sentenced in May 2018 on cybercrime charges following a series of closed proceedings **121** and had been in detention since his arrest in 2017 for "spreading sectarianism and hatred on social media," **122** after calling on Twitter for the release of human rights activist Osama al-Najjar. **123** During his arrest, 12 security officers searched Mansour's house for electronic devices, confiscating laptops and cell phones belonging to him as well as his family members. **124** Activists said he was held in solitary confinement, and was not given access to a lawyer during his trial. **125** As of February 2020, Mansour was

reported to have been on a five-month liquid only hunger strike to protest prison conditions, torture, denial of visitation, and to demand a fair trial (see C7). **126**

Nasser bin Ghaith—a human rights activist and former lecturer at the Abu Dhabi branch of the Paris-Sorbonne University— was sentenced to 10 years in prison in 2017 after being convicted on a range of charges primarily related to his nonviolent speech published online. **127**

In April 2020, three men were arrested in separate incidents for “mocking stay-at-home and movement restrictions” and their pictures were published in the press. Authorities said they were notified of their posts as a result of the “name and shame” initiative started by the Dubai Police. **128** The initiative is used by authorities in Dubai to punish those who mock the ‘stay home, stay safe’ campaign on social media by identifying and shaming violators on mass media and on social media channels run by the Dubai Police. **129** In the same month, Tariq Mehyyas, an Emirati member of the media, was arrested under hate crime charges for posting racist comments in a video targeting South Asian residents of the UAE. **130**

In March 2020, an American woman who was arrested for insulting her ex-boyfriend over email was released after a month in detention on cybercrime charges. UAE cybercrime law prohibits anyone from insulting others in any electronic format. **131**

Citizens continued to be arrested for content they posted online during the reporting period. In May 2019, a man was arrested in Dubai for filming and posting a viral video of a dispute between a hotel worker and a woman after she refused to pay for valet parking service. He faced charges under Article 21 of the cybercrime law for violating the privacy of others, which is punishable by up to six months in

prison and a 500,000 dirham (\$136,000) fine. As of June 2020, he was still being detained. **132** In March 2019, a man was arrested for insulting local traditions after posting a satirical video on social media, in which he wore formal Emirati clothing while surrounded by women and throwing money around. **133** His arrest may have been the result of user reporting. **134** In January 2020, a man was fined 10,000 dirhams for posting a photoshopped picture of another man as a dog. The court also shut down his Instagram account and confiscated his phone. **135**

In November 2019, Abu Dhabi public prosecutors released figures showing that they have handled 512 cases of social media violations in 2019 compared to 357 cases reported in 2018. In 2017, a total of 392 cases of social media abuse were registered. They cited reasons such as online harassment, extortion, threats and blackmail, false information, violating the privacy of others, abusive comments, fake advertisements and rumors, swearing, defamation, inciting others to commit crimes, and fraud. **136**

In July 2018, the Abu Dhabi prosecutor's office issued an arrest warrant for three social media influencers who had participated in a viral dance challenge involving moving vehicles and posted it on social media. They were charged with putting people's lives at risk and promoting "practices that are incompatible with the UAE's values and traditions."

**137**

Several foreigners were arrested for social media posts under the harsh cybercrime law. In April 2019, a British woman was arrested at an airport in Dubai for insulting Facebook comments she posted about her ex-husband's new wife. She was detained under the cybercrime law and released after paying a 3,000 dirham (\$816) fine. **138**

Even after serving their sentences, many prisoners of

conscience remain imprisoned in “counselling centers.” **139** For example, Osama al-Najjar remained in detention in a counselling center despite having served out his three-year sentence. **140** Al-Najjar was finally released from detention in August 2019. **141** He was sentenced to three years in prison and fined \$136,000 in 2014 for tweets alleging that his father, who was imprisoned during the UAE 94 trial (in which 94 democracy activists were tried on trumped up coup charges in 2013), was tortured by security forces. **142** He was found guilty of belonging to the banned political group al-Islah, spreading lies, and instigating hatred against the state through Twitter. **143** He was released in August 2019, after the reporting period. **144**

#### **C4** 0-4 pts

<b>Does the government place restrictions on anonymous communication or encryption?</b>	<b>1/4</b>
---	------------

A number of laws limit anonymous communication online. Amendments to the cybercrime law passed in 2016 state that “whoever uses a fraudulent computer network protocol address (IP address) by using a false address or a third-party address by any other means for the purpose of committing a crime or preventing its discovery” can face a fine of between 500,000 (\$136,000) and 2 million dirhams (\$544,000), as well as prison time. **145** The clause may refer to VPNs used to circumvent censorship, which help disguise the user’s location. A prison sentence was not specified in the law. However, considering that cyber violations are now treated as crimes rather than misdemeanors, prison terms for those convicted would likely be at least three years. **146** The TRA clarified that “companies, banks, and institutions are not prohibited from using VPNs,” adding that “the law can be breached only when internet protocols are manipulated to commit crime or fraud.” **147** Also in 2016,

authorities blocked the encrypted messaging app Signal. **148**

In 2014, the Ministry of Interior announced plans to link identification cards with internet and mobile service “to crack down on child abusers.” An official stated: “By linking ID cards with internet service providers, people’s identities will be linked to the websites they visit.” **149** In order to retain service, mobile phone users were required to reregister personal information as part of the 2012 TRA campaign “My Number, My Identity.” **150** Cybercafé customers are also required to provide their ID and personal information. **151**

**C5** 0-6 pts

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

**0/6**

State surveillance is widespread and infringes on users’ right to privacy. It is unclear whether there is any meaningful legal oversight of government surveillance operations.

In December 2019, the *New York Times* reported that the VoIP app “ToTok” gives UAE spies access to citizen’s conversations, movements, and other personal information like photos. Shortly after, the app was removed from both the Apple store and the Google Store (see B2). The app’s publisher, Breej Holding Ltd, is affiliated with UAE-based cybersecurity firm DarkMatter, which is allegedly under investigation by the United States’ Federal Bureau of Investigation for possible cybercrimes. **152** The founders of the app issued a statement saying that the allegations of ToTok being used for espionage were “vicious rumors.” **153**

A Reuters investigation published in January 2019 revealed that a group of former US intelligence agents were part of Project Raven, an Emirati hacking program that allowed the

UAE to surveil militants and other governments, as well as dissidents, political opponents, activists, and journalists. Some of the latter targets were foreigners. The project was ultimately transferred from a US contractor to DarkMatter in 2016. **154** One of the tools used from 2016 to 2017 enabled DarkMatter to hack into targets' iPhones and access their information. The UAE had also bought the platform, called Karma, from an unnamed vendor. **155** The project operatives were ordered to monitor social media platforms and target individuals who, according to security forces, had insulted the government. One of the operatives said, "Some days it was hard to swallow, like [when you target] a 16-year-old kid on Twitter." **156**

In August 2018, Google said that its Chrome and Android browsers would mark all websites that had been certified by the UAE security firm DarkMatter as unsafe. **157** In July 2019, Mozilla said it was "rejecting the UAE's bid to become a globally recognized internet security watchdog, empowered to certify the safety of websites for Firefox users." Mozilla made the decision based on reports that cybersecurity firm DarkMatter had been linked to a state-run hacking program. **158**

In February 2018, Faisal al-Bannai, the founder of DarkMatter, denied activists' allegations that the firm was involved in hacking activities. About 80 percent of DarkMatter's customers are UAE government agencies, including the Dubai police. Al-Bannai has suggested that the police are capable of compiling hours of surveillance video in order to track anyone in the country. **159** In October 2019, al-Bannai announced that he is "in the process of concluding purchase agreements with multiple parties to divest all assets and capabilities in the UAE and internationally." **160**

Moreover, documents leaked in August 2018, which were

used in two lawsuits against the Israeli technology company NSO Group, showed that the UAE had been using NSO's Pegasus spyware for at least a year against foreign government figures, journalists, and activists. Pegasus can be covertly installed on a person's smartphone after they have clicked on a malicious link, giving hackers access to information on the device. **161**

In 2016, a Danish newspaper revealed that a Danish subsidiary of the British defense contractor BAE Systems was selling surveillance equipment to UAE officials. The equipment was reportedly capable of deep packet inspection (DPI), "IP monitoring and data analysis" for "serious crime," and "national security" investigations. **162** Moreover, in 2015 the UAE government signed a contract with an Israeli surveillance company to launch the so-called Falcon Eye project, a powerful, countrywide surveillance project also known as the Abu Dhabi Safe City. **163**

In 2016, an official from the Dubai police said authorities monitor users on 42 social media platforms. **164** A TRA official also stated, "We have started monitoring all the social media channels—all websites and profiles are monitored." **165**

## C6 0-6 pts

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

0/6

ISPs and mobile service providers are not transparent about the procedures authorities use to access users' information. Service providers reportedly monitor content on behalf of the police and security forces. Etisalat is required, through its license, to store call logs and possess equipment that allows the TRA to access "its network and the retrieval and

storage of data for reasons of public interest, safety, and national security.” **166** Metadata and call information from the VoIP services offered by Etisalat and Du can be obtained by the government. **167**

In its transparency report covering July to December 2018, Facebook reported receiving eight requests for users’ data, three of which were emergency requests, while five were made through the standard legal process. **168** Two requests were made to Google and three to Twitter during the same period. **169**

### C7 0-5 pts

<p><b>Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?</b></p>	<p><b>2/5</b></p>
---	-------------------

Some online activists face enforced disappearances and torture in retaliation for their activities. **170** Nasser bin Ghaith, who was sentenced to 10 years in prison in part for tweets critical of the Egyptian government, reported that he was detained in poor conditions and subject to torture while on trial, including extended periods in solitary confinement. **171** He has gone on several hunger strikes since 2017 (see C3) and has been denied access to medical care. **172**

Activist Ahmed Mansour, who was detained in 2017 in connection with his social media use and later sentenced to 10 years’ imprisonment in May 2018 (see C3), began a hunger strike in March 2019 to bring attention to his case and substandard prison conditions. **173** As of February 2020, Mansour was reported to have been on a five-month liquid only hunger strike (see C3). **174** He had also been harassed for years by the government prior to his imprisonment. Authorities froze his bank accounts, put him under a travel

ban, denied him a passport, and attempted to hack into his email accounts. When arresting him, security forces searched Mansour's house and confiscated all electronic devices belonging to him and his family members. **175**

Political dissidents and their families are frequently harassed and intimidated via Twitter. In December 2019, Human Rights Watch reported that dissidents and their family members report being targeted and surveilled. They are constantly summoned and interrogated for their opinions, intimidated, and asked to spy on their communities. **176** In October 2019, Amnesty International shared a statement by WhatsApp about an NSO spyware which was sent via the chatting app to 100 activists in the UAE, Mexico, and Bahrain. **177**

**C8** 0-3 pts

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

Activists have faced repeated technical attacks designed to deceive them into downloading spyware. In May 2019, reports emerged that NSO Group, whose spyware enabled various countries to surveil journalists and activists, exploited a security flaw in WhatsApp to hack into targets' mobile devices. The flaw may have been used to hack the UAE's targets. **178** In 2016, a report from the *New York Times* asserted that the UAE government paid the Italian cybersecurity firm Hacking Team more than \$634,000 to target 1,100 devices with spyware. **179** Through a forensic investigation by cybersecurity expert Bill Marczak, human rights activist Ahmed Mansour discovered that he had been repeatedly targeted with sophisticated spyware from

hackers at FinFisher and Hacking Team.

A January 2019 Reuters report documented how former United States intelligence analysts are now working as hackers within the UAE as part of a clandestine spy group called Project Raven, which was then moved to the UAE cybersecurity firm DarkMatter (see C5). These hackers use state-of-the-art technology to hack into phones and spy on enemies of the state, including journalists, activists, and political rivals. **180**

In 2016, Citizen Lab helped Mansour investigate a link he received in an SMS, which was a “sophisticated piece of malware that...would have allowed the attackers to get full control of Mansour’s iPhone.” The spyware was provided by NSO Group. **181** Another report by Citizen Lab demonstrated five cases where arrests or convictions of users followed malware attacks against their Twitter accounts from 2012 to 2015. **182**

In June 2019, the Minister of State Anwar Gargash said at a media roundtable that his government doesn’t spy on its own citizens, and that he doesn’t know how much the country spends on cyberweaponry. Gargash then added: “We have a policy, also, not to talk about the details of cyber.” **183**

In February 2020, a trial in London began in which Farhad Azima, an Iranian-American businessman, alleged that the Emirate of Ras Khaima had hacked his emails, as they battled him over an hotel contract. According to his lawyer, if the judge rules in Azima’s favor, he would be the first person to successfully sue a foreign government for hacking. **184**

In 2016, an official with DarkMatter said that 5 percent of global cyberattacks targeted victims in the UAE. **185** The TRA said it had “successfully foiled 1,054 cyberattacks” targeting

private companies and government entities that year. **186**

Also in 2016, Dubai police arrested foreign hackers accused of blackmailing over email five senior officials who work for the president of the United States. **187**

### Footnotes

**1** International Telecommunication Union, “Percentage of individuals using the internet, Percentage of individuals with mobile-cellular subscriptions,” 2018, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

**2** Telecommunications Regulatory Authority, Spreadsheet, <http://www.tra.gov.ae/userfiles/assets/OY5gNo6smIP.xlsx>

**3** International Telecommunication Union, “Percentage of individuals using the internet, Percentage of individuals with mobile-cellular subscriptions,” 2018, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

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

Join the Freedom House monthly newsletter

Email



**4** “Etisalat 5G service launch in UAE,” Tech Radar, <https://www.techradar.com/news/etisalat-5g-service-and-smartph...>

**5** Cleofe Maceda, “Du launches 5G service in UAE, giving away free phones to select customers,” Gulf News, June 2, 2019, <https://gulfnews.com/business/du-launches-5g-service-in-uae-giving-away...>

More footnotes

#### ADDRESS

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

#### GENERAL INQUIRIES

[info@freedomhouse.org](mailto:info@freedomhouse.org)

#### PRESS & MEDIA

[press@freedomhouse.org](mailto:press@freedomhouse.org)

@2020 FreedomHouse