**Key Developments: June 2015 – May 2016**

- Authorities issued blocking orders against several overseas news websites over the past year, including *Middle East Eye*, *The New Arab*, and *al-Araby al-Jadeed* for unfavorable coverage of the country’s human rights abuses. Two Iran-based news sites were also blocked in a reflection of mounting tensions between the two countries (see *Blocking and Filtering*).

- A July 2015 law designed to combat discrimination and hate speech also outlines jail terms of six months to over 10 years and fines from US$ 14,000-550,000 for online posts deemed to insult “God, his prophets, apostles, holy books, houses of worship, or graveyards” (see *Legal Environment*).

- In June 2015, Nasser al-Faresi was sentenced to three years in jail for tweets found to have insulted the Federal Supreme Court and the ruler of Abu Dhabi. The court convicted him of “spreading rumors and information that harmed the country” (see *Prosecutions and Detentions for Online Activities*).

- Academic and activist Dr. Nasser Bin Ghaith was arrested and held incommunicado until April 2016, when it was announced he was held on numerous charges, including “committing a hostile act against a foreign state” for tweets that criticized Egypt’s treatment of political detainees (see *Prosecutions and Detentions for Online Activities*).

- Leaked invoices from up until 2015 showed the government paid cybersecurity firm Hack- ing Team over US$ 634,500 to deploy spyware on 1,100 devices (see *Surveillance, Privacy, and Anonymity*).
Introduction

Internet freedom remained highly restrictive in the United Arab Emirates over the past year, with prominent critics imprisoned for political tweets and ordinary users arrested in often absurd circumstances.

The country’s information and communication technology (ICT) industry continues to grow, with the UAE now ranked third among Arab states in the ICT Development Index. However, the telecommunications industry remains tightly controlled by the government, which directly or indirectly owns large stakes in the country’s two service providers. Close ties between the government and telecommunications companies may be a reason for consumer-unfriendly practices, such as restrictions on Voice-over-IP (VoIP), rampant censorship, and pervasive surveillance.

The state blocks access to political, social, or religious content that differs from the state’s narrative, from pornography and gambling to political discussions and LGBT content. Self-censorship is pervasive on social media and state-run news sites generally refuse to cover controversial issues. Despite several laws that routinely violate the right of users to freely express themselves online, the families of political detainees often take to Twitter to highlight human rights abuses and communicate on behalf of their loved ones.

Just as with cybercrime and antiterrorism laws introduced in years’ past, a July 2015 anti-hate speech law includes disproportionate penalties. Users face prison terms of up to 10 years and US$ 550,000 fines for crimes such as insulting religious figures, holy books, and prayer sites. Due to these broad laws and a judiciary that lacks independence, nonviolent opposition activists are sometimes targeted under laws designed for terrorists and cybercriminals. For example, activist and academic Nasser Bin Ghaith has been detained since August 2015 for, among other charges, “committing a hostile act against a foreign state” after tweeting about Egypt’s unfair treatment of political detainees. Meanwhile, both locals and foreigners were arrested or deported for social media posts, often in absurd circumstances. Recent reports revealed how security services have targeted 1,100 devices with sophisticated spyware, reinforcing fears among dissidents that they are being watched.

Obstacles to Access

Emirati users enjoy a robust ICT infrastructure and high connection speeds. However, the major telecom companies are either fully or partially owned by state-owned, resulting in high prices, weak competition, and consumer-unfriendly practices, such as the blocking of popular VoIP services.

Availability and Ease of Access

The United Arab Emirates (UAE) is one of the world’s most connected countries. The number of internet users has risen rapidly from a penetration rate of 68 percent in 2010 to 91 percent at the end of 2015 according to the International Telecommunication Union. As of October 2015, there were 1,163,449 internet subscribers in the country, 99 percent of whom had broadband connections. The UAE has one of the highest mobile phone penetration rates in the region at 187 percent, represent-
The country ranked 32nd in the 2015 Internet Development Index, up from 49th in 2010 and third among Arab States behind Bahrain and Qatar.

While broadband use is widespread, the country has one of the most expensive broadband rates in the world, with high-end subscriptions costing more than AED 8,000 (US$2,178) a year. However, the UAE ranked 22nd in the ITU’s 2014 ICT Price Basket Index, in which local broadband prices are measured against gross national income (GNI) per capita. This reflects a sense that despite the high prices, the internet remains affordable for most Emiratis, though not necessarily to the country’s large population of expatriate workers.

On two recent occasions in September 2014 and April 2015, provider Etisalat upgraded broadband speed for 100,000 business clients. In November 2015, broadband speeds were doubled for home customers at no extra charge. In January 2016, provider Du announced upgraded internet speed for its home users. In addition, the Emirates is set to be the first country to see a nation-wide rollout of the 5G network in time for the Expo 2020 exhibition.

According to UNICEF, literacy in the Emirates was reported at 94 percent among males and 97 percent among females, and thus does not constitute a strong obstacle to internet use. Emirati schools are now among the top 25 worldwide for online connectivity. There are over 200 smart-learning schools, compared with only 14 in 2012. The program currently benefits 34,513 students, who are also equipped with tablets as part of the scheme. Principals are also enrolled in international computer literacy training programs. By 2017, the country expects its Smart Learning Program to be installed in all K-12 government school classes, replacing textbooks with tablets and allowing students to interact with educators through an online platform.

Restrictions on Connectivity

Most popular Voice-over-Internet-Protocol (VoIP) services are restricted over mobile connections. Etisalat and Du are the only two operators licensed to provide VoIP services, which are costlier than international alternatives. Snapchat’s new voice and video calling feature was blocked upon its introduction.

---

launch in April 2016. Similarly, WhatsApp's voice feature was blocked shortly after it was introduced in March 2015. Two months after that, Facebook's video-calling feature was also blocked. Similar products such as Viber or Apple's Facetime have been banned since 2013; in fact, Apple agreed to sell its iPhone products to UAE mobile phone companies without the Facetime application preinstalled. Users in the UAE reported that Skype and Viber only work over Wi-Fi and Apple's Facetime video-calling feature can only be used if the iPhone was purchased outside the country.

Despite these limitations, circumvention software and proxies are commonly used by Emiratis to access blocked content and VoIP services. Due to a UAE law that specifically criminalizes the use of VPNs in order to commit illegal activities, there have been fears that using VoIP services through VPNs could be punishable by law.

There were no known government orders to shut down ICT connectivity over the coverage period. However, internet service providers (ISPs) in the UAE are either fully or partially owned by the state, allowing for authorities to exert control over the flow of information in the country. Seeking to improve connectivity within the country, the country's two internet service providers—Etisalat and Du—have launched their own carrier-neutral international internet exchange points, Smarthub and Datamena, respectively. Etisalat maintains its nationwide fiber optic backbone, while in May 2015 the company selected TeliaSonera International Carrier (TSIC) as its preferred global internet backbone provider under a framework deal.

Cuts to undersea cables have disrupted internet access for Emirati users on several occasions, though government-instituted outages are not known. In January 2016, Du warned customers of slower internet due to cuts at three submarine cable operators – EIG, FEA and Falcon.

**ICT Market**

Both Etisalat and Du are, directly or indirectly, owned by the state. The UAE government maintains a 60 percent stake in Etisalat through its ownership in the Emirates Investment Company, while a majority of Du is owned by various state companies. Du pays a percentage of its profit and revenue as a dividend to the UAE federal government, which owns 39.5 per cent of the telecom operator
through its sovereign wealth fund the Emirates Investment Authority. In June 2015, the government announced a decision to allow up to 20 percent of Etisalat shares to be held by foreign investors. The two companies are also the major mobile phone operators.

Regulatory Bodies

Providers fall under the laws and regulations set by the Telecommunications Regulatory Authority (TRA). The authority was established in 2003 and is responsible for the management of “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 IT services within the UAE, resolving disputes between the licensed operators, establishing and implementing a regulatory and policy framework, and promoting new technologies.

In March 2015, the TRA and Dubai police launched the “Digital Blackmail” campaign calling on users to report incidents of cybercrime and blackmauling, which are punished with up to ten years in jail. An official from the Department of Cybercrime at Dubai Police said the police handled 1,820 cyber-crimes in 2015, 239 more than 2014. Following up from its “My Number, My Identity” campaign launched back in June 2012, the TRA called on users to “reregister their SIM cards before documents expire” to avoid cancellations. The authority said the move was “the result of studies that suggested an increase in civil and criminal cases related to the misuse of SIM cards.”

Limits on Content

Authorities keep strict control over the online media landscape, blocking websites that criticize the government or tackle social taboos. Self-censorship is pervasive on social media and state-run news sites refuse to cover controversial issues. Nonetheless, the families of political detainees often take to Twitter to highlight human rights abuses and communicate on behalf of their loved ones, at great risk to their safety.

Blocking and Filtering

Over the past year, the UAE blocked several overseas news websites for content that ran against the state’s political narrative. The UK-based, English-language news site Middle East Eye was blocked in December 2015 after it published articles exposing the country’s harsh surveillance practices and poor human rights record. That same month, authorities blocked the Arabic-language news site al-Araby al-Jadeed and its English equivalent The New Arab, both based in the UK and funded by

---


www.freedomonthenet.org
Qatar, although the sites were unblocked in February.\(^{34}\) News agencies based in Iran, such as Fars News and Al Alam TV, had their Arabic-language sites blocked during the coverage period over allegations they disseminated antigovernment propaganda, according to the Arabic Network for Human Rights Information.\(^{35}\)

The TRA instructs ISPs to block content related to terrorism, pornography, and gambling, as well as websites that contain political speech threatening to the ruling order. However, in reality, the UAE censors a wide variety of topics. Although YouTube, Facebook, Twitter, and international blog-hosting services are freely available, controversial terms are often filtered from search results within these sites. According to Herdict, the crowdsourcing tool that lets users report blocked content, internet users from the UAE have reported several social, political, LGBTQ, dating, and proxy sites are blocked.\(^{36}\) In December 2014, a website run by anonymous employees of Emirates airlines was reported to be blocked in the country.\(^{37}\) The website of Beirut-based NGO Gulf Center for Human Rights was blocked in January 2015.\(^{38}\) On Reddit, users reported the blocking of archive.today, a tool that keeps snapshots of URLs entered in case content disappears or gets modified.\(^{39}\) iHerb.com, an online retailer of nutritional supplements and wellness products, was reported to have been banned in June 2015.\(^{40}\) Worldstar, a website for entertainment and media news, was reported blocked in November 2015,\(^{41}\) as well as the Arabic entertainment website Akoam.\(^{42}\) Twitter’s livestreaming app Periscope was blocked for 48 hours in August 2015 reportedly due to a technical problem, according to a tweet by the TRA.\(^{43}\)

Using the hashtag #blocked_sites_in_uae, blogger and human rights activist Ahmed Mansoor has asked users to help reveal which websites are being blocked. Users have reported the blocking of Twitter hashtags relating to political detainees,\(^{44}\) as well as sites related to the Muslim Brotherhood and regional NGOs.\(^{45}\) Arabic websites and political blogs such as Noonpost, Sasapost, Arabi21, and twsela.com were all reportedly blocked in 2015-16.\(^{46}\) Skype’s download page and online forum continued to be blocked during the coverage period, alongside several proxy websites. Earlier in 2015, the dating app Tinder was blocked.\(^{47}\)

The Lebanese queer and feminist e-magazine Bekhsoos\(^{48}\) and the U.S.-based Arab Lesbian e-magazine Bint El Nas are both blocked.\(^{49}\) Many websites displaying religious content are blocked, includ-


\(^{37}\) Blog no longer active: [Emirati Illuminati](http://www.emirates-illuminati.org/uae-blocks-emirates-illuminati/).


\(^{41}\) See [https://twitter.com/DIJICH/status/660862153184841728](https://twitter.com/DIJICH/status/660862153184841728).


\(^{44}\) Salloh, Twitter Post [in Arabic], May 5, 2015, 7:01 AM, [http://bit.ly/1hGqQy](http://bit.ly/1hGqQy).


\(^{46}\) See [https://twitter.com/search?f=tweets&vertical=default&q=%23blocked_sites_in_uae%20&src=typd](https://twitter.com/search?f=tweets&vertical=default&q=%23blocked_sites_in_uae%20&src=typd).


ing an Arab-Christian online forum named The Church Network. A number of secular and atheist websites and forums in Arabic continue to be blocked such as 3almani.org, secularkuwait.freeforums.org, nadyelfikr.net, alawan.org, “Modern Discussion,” ladeenyon.net, and ladeeni.net. The Emirati atheist blog of “Ben Kreishan” continues to be inaccessible in the UAE.

Authorities continue to ban inactive sites such as the political forum UAE Hewar and the blogs Secret Dubai Diary and UAE Torture. The latter had posted a torture video taken in 2004 in which a member of the ruling family was shown to have tortured an Afghan man. The suspect was acquitted in 2010 in a case that was widely believed to be a show trial. A request to unblock UAE Hewar was rejected by the Federal Supreme Court in July 2012, and its Facebook page is also blocked due to its criticism of the regime and state corruption. As part of a 2013 verdict in which five users were sentenced to 7 to 15 years on charges of violating the constitution and cooperating with foreign political organizations (see “Prosecutions and Detentions”), a court ordered the blocking of five websites: the Emirates Media and Studies Center (EMASC); the Seven Emirates, which focuses on the seven activists who had their citizenship revoked for their political activities; the California-based Arabic news site Watan; the Islah political group website; and the Yanabeea.net educational network. In January 2016, Watan said the TRA has threatened to sue the company hosting its domain, referring to a “court order against the website.”

In 2013, a website disseminating news of the trial of 94 Emirati political detainees was also blocked. The anonymous website UAE University Watch and UAE Prison, which exposes violations against jailed expatriates, have both been blocked. Emaraty Bedoon, the blog of the stateless individual Ahmed Abdulkhaleq who was deported to Thailand in July 2012 for his political activism, is also blocked. Pages of political significance, such as the Arab-American news website Arab Times and the anonymous Secret Dubai blog continue to be blocked. In January 2014 alone, Twitter users have reported the blocking of ProxTube which unblocks censored YouTube content, the chatting website Omelga, and the image-based social network We Heart It.

The telecommunications company Du details what criteria it uses to block websites in a document available on its website. Prohibited content includes information related to circumvention tools, the

---

50 Arab Church, http://www.arabchurch.com/.
52 “Help us document blocked Internet Sites in UAE,” http://bit.ly/1e00dvW.
53 Secret Dubai diary (blog), http://secretdubai.blogspot.com/.
61 UAE University Watch, http://www.uaeuniversitywatch.net/.
63 Emaraty Bedoon (blog), http://www.emaratybedoon.blogspot.com/.
promotion of criminal activities, the sale or promotion of illegal drugs, dating networks, pornography, homosexuality, gambling, phishing, spyware, unlicensed VoIP services, terrorism, and material that is offensive to religion. 66 No similar list was made available by Etisalat, although the company does have a space on its website where users can request that a website be blocked or unblocked. 67 In 2005, an Etisalat spokesman clarified that the company is not responsible for internet blocking and revealed that all complaints and requests are passed on to the Ministry of Information. He also claimed that a list of websites to be blocked is compiled by an American company and then implemented through a proxy server. 68 According to a report from Citizen Lab in January 2013, ISPs in the UAE have used tools such as SmartFilter and NetSweeper to censor content. Citizen Lab also found five installations of Blue Coat ProxySG in the country’s network linked to Etisalat. 69 Another report from CitizenLab in November 2013 listed websites that are blocked in the UAE because both SmartFilter (used by Etisalat) and NetSweeper (used by Du) have miscategorized them as nudity or pornographic content. 70

When Twitter users have complained about a site being wrongfully blocked, Etisalat and Du responded by asking users to complete an unblocking request via online forms. However, neither provide information on whether bans have been lifted in response to such requests. 71 In May 2015, Twitter users reported the blocking and later unblocking of the social platform Wattpad. 72 Similarly, Emirati columnist Sultan al-Qassemi noted the unblocking of the news website The New Arab in February. 73 The TRA has also called on users to help report “suspicious” content for blocking.

The TRA, working with the Ministry of Communications, blocks at least five hundred search terms. 74 The TRA claimed the number of blocked websites is unknown “due to the nature of blocking operations”. 75 In a previous statement, TRA stated that 82 percent of the websites blocked during the period from January to March 2015 were blocked for nudity and dating content, 8 percent for violating UAE laws, and 9 percent for containing phishing, hacking, and spyware content. 76

**Content Removal**

The removal of online content often lacks procedural transparency or judicial oversight. Under the 2012 cybercrime law, website owners and employees “may be held liable” for any violations occurring on their sites, including defamation charges. 77 An official from the TRA stated in 2015, “We try

---

71 See Etisalat_Care, Twitter Post, December 30, 2015, 5:52 AM, [http://bit.ly/1LmIQD2](http://bit.ly/1LmIQD2); and [https://twitter.com/dutweets/status/414787641620430848](https://twitter.com/dutweets/status/414787641620430848) [offline].
72 See [https://twitter.com/MayraRahab/status/596619001272209408](https://twitter.com/MayraRahab/status/596619001272209408).
73 See [https://twitter.com/SultanAlQassemi/status/704050010003021828](https://twitter.com/SultanAlQassemi/status/704050010003021828).
to get the page or profile down or remove the violation as soon as possible and report the case to
police if it is a criminal case.”

According to Google’s Transparency Report for the second half of 2015, the company received a
request from the TRA to remove a YouTube video showing an Emirati royal family member torturing
Sudanese workers at his farm. The company did not remove the video out of respect for the public
interest. In 2014, Google had reported two requests from the UAE to remove Google+ posts that
violated the 2012 cybercrime law. The posts were blocked locally because they “contained obscene
language and political satire against members of the ruling family of the UAE.”

Twitter received one removal request from the UAE over the coverage period and did not withhold
any content in response. In November 2015, Dubai Authorities reported the termination of 202 Insta-
gram accounts and 218 websites “for selling and promoting fake products.”

Media, Diversity, and Content Manipulation

In addition blocking and content removal, Emirati authorities also use financial means to limit the
ability of antigovernment websites to produce content online. For example, the government report-
edly pressured Dubai-based advertising agency Echo to end its advertising contract with the U.S.-
based news outlet Watan. A complaint was also allegedly submitted to the FBI against the website,
claiming it calls for the assassination of UAE rulers. Nonetheless, users have access to a variety of
local and international news outlets, even if there are disparate reports of the blocking of specific
UAE-related articles from these sites.

Local news websites, many of which are owned by the state, employ a large degree of self-censor-
ship in accordance with government regulations and unofficial “red lines.” Gulf News, The Nation-
al, and Emirates 24/7 are among the different online media outlets facing restrictions. The overall
press freedom environment in traditional media is dire, with foreign journalists and scholars often
denied entry or deported for expressing their views on political topics. In February 2016, the Fed-
eral National Council passed a bill regulating responsibilities of the new National Media Council, a
federal government body affiliated with the cabinet that “has a corporate character and a mandate
to undertake the responsibilities of overseeing and supervising media in the UAE.”

transparencyreport/removals/government/notes/?hl=en#authority=AE
81 Twitter’s Transparency Report is available at https://transparency.twitter.com/en/removal-requests.html#removal-requests-
jan-jun-2016.
82 “Dubai shuts down 202 Instagram accounts for promoting fake goods,” Emirates 24/7, November 4, 2015.
83 ANHRL “UAE Continues its Serious Violations Against the Freedom of Opinion and Expression due to Blocking “Watan”
Vartanian, “Artist Walid Raad Denied Entry into UAE, Becoming Third Gulf Labor Member Turned Away,” Hyperallergic, May 14,
http://bit.ly/1Oxn2JH.

www.freedomonthenet.org
be responsible for proposing regulations and “accrediting media outlets and their staff and activities including e-publishing.”

Nonetheless, since the regional uprisings of 2011, Emiratis have begun to tackle sensitive issues more boldly over the internet, particularly on social media. Users express their opinions, share information on arrests and trials, and even attempt to organize protests. However, most users remain anonymous when criticizing state officials or religion out of fear of legal action or harassment. In 2014, The United Arab Emirates spent more than $12 million on public relation firms, which some observers suspect have been deployed to counter negative images of the country’s human rights abuses online. A large number of anonymous Twitter users appear dedicated to harassing and intimidating political dissidents and their families online.

Digital Activism

Some Emiratis have continued to push back against government repression and intimidation by channeling their strong digital literacy into online activism, writing blogs, and calling for political reform on social networks. In the face of prosecution, activists still use online tools to highlight human rights violations and pass on messages from relatives in prison. Families of political prisoners still rely on Twitter to speak on behalf of detainees, explaining their cases, spreading information about violations of their rights, and calling for their release. There are several examples of relatives who are active online, including Mariam al-Mansouri, the wife of detained blogger Rashid al-Shamsi, and Aysa al-Thufiri, the daughter of detainee Salih al-Thufiri. Nonetheless, the online environment in the UAE is not free, and users face many challenges to freedom of expression online. For instance, three sisters were secretly detained for three months for tweets calling for the release of their detained brother Issa al-Suwaidi.

Violations of User Rights

Several laws, including the penal code, the publishing law, and the cybercrime law, are commonly exploited to deter free expression and violate the rights of users. Several prominent online activists were jailed over the coverage period, while both locals and foreigners were targeted for social media posts, often in absurd circumstances. Finally, there is a general feeling among those who reside in the UAE that online tools are monitored and that surveillance is widely practiced with little judicial oversight.

Legal Environment

Article 30 of the UAE constitution states that “Freedom of opinion and expressing it verbally, in writing or by other means of expression shall be guaranteed within the limits of law.” However, the Emi-

---

88 Marian Mansori, Twitter Account, https://twitter.com/MariamMansori.
89 Aysha_75, Twitter Account, https://twitter.com/Aysha_75.
rati judicial system lacks independence, and prosecutions are often pursued for political reasons. Since the 2011 uprisings throughout the region, the countries making up the Gulf Cooperation Council made a collective effort to pass legislation criminalizing criticism of the authorities.

Several legislative amendments further restricted free speech, particularly on sensitive topics such as religion. Citing the need to curb hateful rhetoric and promote tolerance in order to defend against terrorism, authorities passed Federal Decree Law No. 2/2015 in July 2015. However, several provisions in the law go beyond the punishment of hate speech or incitement to violence. By including insults to “God, his prophets or apostles or holy books or houses of worship or graveyards,” the law paved the way for further punishment of individuals for expressing nonviolent opinions on religion. Penalties under the law range from jail terms of 6 months to 10 years and/or fines of AED 50,000 to 2,000,000 (approximately US$ 14,000 to 550,000). Furthermore, while the law’s scope 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. The law specifically includes speech made over online media.

Amendments to the cybercrime law were proposed this February and later passed July 2016 as Federal Law No. 12/2016. The act of using “a fraudulent computer network protocol address” in order to “commit a crime or prevent its discovery” was raised from a misdemeanor to a crime now punishable by temporary imprisonment, and fines were raised from AED 150,000–500,000 to AED 500,000–2,000,000. While the cybercrime law provided a sounder legal basis to combat online fraud, money laundering, hacking, and other serious cybercrimes, the law also criminalized a wide range of online activity commonly accepted within international norms. For example, hefty fines and jail sentences await users who engage in online gambling, disseminate pornographic material, or violate another person’s privacy through posting their photograph or making statements about them online, regardless of the accuracy of the accusations. Intermediaries, such as domain hosts or administrators, are also 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.” The cybercrime law also contains punishments for offenders other than its symbols, or for insulting Islam and other religions. Calls to change the ruling system are punishable by life imprisonment. Authorities have repeatedly warned foreign nationals that they must also follow the country’s restrictive laws.

The Terrorism Law No. 7, passed in 2014, includes punishments such as life imprisonment, death, and fines up to AED 100 million (US$27 million) for terrorism offenses. 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.”

Articles 8 and 176 of the penal code are used to punish public “insults” against the country’s top
officials, although these articles are also widely used to prosecute any users that express a desire
for political reform. Articles 70 and 71 of the 1980 publishing law prohibit criticism of the head of
the state and of Islam or any other religion. In February 2016, Dubai police reiterated that posting
pictures of others without permission can lead to six months in jail and a fine between AED 150,000
and 500,000 (USD 41,000 and 136,000).

Several court decisions over the past year negatively impacted internet freedom. In June 2015, the
Federal Supreme Court ordered the retrial of an individual for making insults over WhatsApp mes-
gages, increasing the original fine of AED 3,000 (around US$ 800) to AED 250,000 (US$ 68,000), as
well as ordering his/her deportation. Later, in December 2015, Dubai’s Court of Cassation over-
turned a lower court’s acquittal in a defamation case over a Facebook posting. The lower court had
acquitted the defendant based on the fact that his post was in a private Facebook group that was
not accessible to the general public. However, the prosecutor successfully appealed the verdict, ar-
uing that “even if the Facebook page is not accessible to general public, posting derogatory com-
ments defames a person and damages his or her reputation.” The defendant, who is accused of
insulting a woman on Facebook, will now have his case reheard by a new panel of judges.

Prosecutions and Detentions for Online Activities

The UAE routinely jails individuals for posting political, social, or religious opinions online. Numerous
incidents were witnessed over the coverage period, while several individuals remain behind bars
from lengthy prison sentences past in previous years.

Several Emiratis were sentenced to prison over the coverage period for criticizing state institutions:

- In August 2015, Dr. Nasser Bin Ghaith was arrested and held in arbitrary detention until
  April 2016, when it was announced he was held on numerous charges, including “commit-
  ting a hostile act against a foreign state” for tweets that criticized the Egyptian judiciary’s
  treatment of political detainees. Bin Ghaith, who remained in detention as of late 2016, is
  a human rights activist and former lecturer at the Abu Dhabi branch of the Paris-Sorbonne

  middle-east-33152898.
nation/crime/mans-acquittal-over-fb-post-reversed.
107 Ryan Stultz, “Dubai court rules even ‘private’ Facebook posts subject to prosecution,” Stepfeed.com, December 8, 2015,
  V7kYkZIMrL8.
108 “Free Emirati human rights defender Dr. Nasser Bin Ghaith, on trial for online posts in violation of his right to free
University.\textsuperscript{109} He was previously arrested in 2011 for signing an online petition demanding political reform.\textsuperscript{110} His trial has been repeatedly adjourned and he states he was tortured while in detention, for which authorities have also charged him with damaging the reputation of the UAE.\textsuperscript{111}

- In June 2015, Nasser al-Faresi was sentenced to three years in jail for a tweet insulting the Federal Supreme Court and the ruler of Abu Dhabi. The court charged him with “spreading rumors and information that harmed the country.”\textsuperscript{112}

Several foreigners were also targeted for social media posts under the country’s harsh cybercrime laws:

- Jodi Magi, an Australian national, was fined AED 10,000 (US$2,700) and deported in July 2015 after posting a picture to Facebook showing her neighbor’s vehicle parked across two parking spaces reserved for the disabled.\textsuperscript{113} Magi was found to have violated the cybercrime law by taking photos without the consent of the vehicle’s owner as well as using offensive remarks against the owner.\textsuperscript{114}

- In January 2016, the Federal Supreme Court sentenced a Palestinian man to three years in jail and a fine of AED 50,000 (US$13,500) for “insulting the UAE on social media.” The man, who pleaded not guilty, told the judge the incident in question was a private interaction with another Facebook user.\textsuperscript{115}

- In March 2016, an Omani man was sentenced to three years in jail and fine of AED 50,000 (US$13,500) for describing UAE soldiers killed in Yemen as “cowards” over WhatsApp messages. He will be deported after serving his sentence.\textsuperscript{116}

Other cases from the coverage period include:

- In March 2016, Marwan Mohamed Ateej was sentenced to five years imprisonment and a fine of AED 1,000,000 (US$272,000) for online posts in support of the Muslim Brotherhood. Court documents claimed he “legitimised [sic] the work of the Muslim Brotherhood calling them peaceful, unarmed heroes and rallied on people to support them.”\textsuperscript{117}

- In June 2016, the Abu Dhabi Court sentenced an expat man to six months in jail and an AED

\textsuperscript{112} Reuters, “UAE man jailed for tweets critical of high court: newspaper,” Yahoo! News, June 30, 2015, http://yhoo.it/1VUf0cJ.
\textsuperscript{116} “Man jailed for insulting UAE on WhatsApp,” Arabian Business, March 1, 2016, http://www.arabianbusiness.com/man-jailed-for-insulting-uae-on-whatsapp-623405.html#V7k0RJMrLBL.
\textsuperscript{117} Naser al Remeithi, “Man jailed for five years for supporting Muslim Brotherhood,” The National, March 27, 2016, http://www.thenational.ae/uae/courts/man-jailed-for-five-years-for-supporting-muslim-brotherhood.
50,000 (US $13,500) fine for uploading torrents to a pirate streaming website. He will also be deported after serving his sentence.\textsuperscript{118}

- In April 2016, an Emirati woman was tried for insulting her maternal uncle and his religious sect over WhatsApp. The woman pleaded guilty and, under the antidiscrimination law, could face a minimum five years in jail and/or a fine that ranges between AED 500,000–1,000,000 (US$ 135,000–272,000).\textsuperscript{119}

- In January 2016, two men were briefly arrested and questioned for posting a selfie in front of a Dubai hotel which had caught fire.\textsuperscript{120}

- In January 2016, two Emirati soldiers were arrested after a video of them performing a Saudi hip-hop dance went viral. The two were charged with disrespecting the UAE army and its uniform.\textsuperscript{121}

Numerous Emirati users continue to serve long prison sentences for their online activities, mainly related to the UAE94 trials directed against alleged members of the banned opposition movement al-Islah.\textsuperscript{122}

- Blogger Khalifa Al-Nuaimi\textsuperscript{123} and Twitter users Rashid al-Shamsi\textsuperscript{124} and Musabeh al-Rumaithy\textsuperscript{125} were arrested for their online activities and sentenced to 10 years imprisonment in July 2013.

- Blogger Abdullah al-Hajri\textsuperscript{126} and Twitter user Omran al-Radhwan\textsuperscript{127} are serving seven-year sentences.\textsuperscript{128}

- In November 2014, online activist Osama Al-Najjar was sentenced to three years in prison and fined US$136,000 for tweets alleging that his father, who was imprisoned as part of the UAE94 trials, was tortured by security forces.\textsuperscript{129} He was found guilty of belonging to...
the banned political group al-Islah, spreading lies, and instigating hatred against the state through Twitter.130

- Abdulrahman Bajubair was sentenced to five years in jail for running a blog and Twitter accounts reporting on the mistreatment of political detainees in December 2013.131

- In March 2014, Khalifa Rabeiah and Othman al-Shehhi were fined and are currently serving a five-year sentence for tweets critical of the judiciary system.132

**Surveillance, Privacy, and Anonymity**

The high amount of prosecutions and physical harassment of users in the UAE is, in part, due to the obstacles they face in using ICT tools anonymously. Emirati activists have consistently faced spyware attacks. In May 2016, a report from the New York Times stated the UAE government paid the cybersecurity firm “Hacking Team” more than $634,500 to target 1,100 devices with spyware able to track their owners’ activities.133 Through a forensic investigation by cybersecurity expert Bill Marczak, Emirati human rights activist Ahmed Mansoor discovered he had been repeatedly targeted with sophisticated spyware from FinFisher and Hacking Team. A May 2016 report by CitizenLab demonstrated five cases where arrests or convictions of users followed malware attacks against their Twitter accounts from 2012 to 2015.134

Internet and mobile providers are not transparent about the procedures taken by authorities to access their data and users’ information. Incidents of providers demanding warrants or legal permissions for security bodies to gain access to user data are not known. In February 2016, an official from Dubai police said the country monitors users on 42 social media platforms.135 Ghaith Al Mazaina, acting manager at the security quality service at the TRA, stated: “We have started monitoring all the social media channels – all websites and profiles are monitored.”136

Cybercafe customers are also required to provide their ID and personal information.137 In April 2014, the Ministry of Interior announced plans to link ID cards with internet services and cellphones “to crackdown 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.”138 In March 2015, the TRA announced the establishment of an alert system that detects certain keywords relating to “nudity, sexual cyber-extortion and insulting members of the ruling families.” Mobile phone users re-registered their per-

---


sonal information as part of a 2012 TRA campaign “My Number, My Identity.” In January 2013, the country’s two mobile phone providers issued a final warning to their users to register their SIM cards or have their lines cut.

Intimidation and Violence

Online activists in the UAE face arbitrary detention, enforced disappearances, and in some cases torture. In December 2015, Jordanian journalist Taysir al-Najar was detained at the airport before leaving to Jordan for a family visit. As of mid-2016, al-Najar remained in arbitrary detention for a 2014 Facebook comment critical of the authorities. For two months, his family did not know his whereabouts. Omani blogger Muawiyah Alrawahi was arrested as he entered the country by car and held in arbitrary detention for 13 months. He has a vocal critical of both Omani and UAE authorities online. Human rights defender Ahmed Mansoor has faced continual harassment by the authorities, and is subject to a travel ban.

Technical Attacks

The UAE remains one of the top countries facing hacking attempts worldwide. According to a 2015 study by Kaspersky Lab, the UAE is the second most attacked country online in the Middle East and the 15th most attacked worldwide. In January 2016, two foreign men were each sentenced to one year in prison and fined AED 500,000 (US$ 135,000) for hacking into the computer system of a support services company. The duo were found to have divulged secret information to the company’s competitors. In July 2015, several UAE banks were hit by a coordinated cyberattack crippling e-banking operations and websites. That same month, the cybersecurity company Symantec uncovered a new corporate espionage group that has compromised a string of major corporations in recent years, including three organizations located or headquartered in the UAE.

139 The TRA’s statement reads: “Your mobile phone number is an extension of your identity. Sharing or giving away your SIM-Card to others can cause unwanted consequences, including being held accountable for any improper conduct or misuse associated with the mobile phone subscription by the authorities as well as being liable for all charges by the licensees.” Telecommunications Regulatory Authority, “My Number My Identity,” accessed April 28, 2013, http://bit.ly/1LPbs66; and Nadeem Hanif, “Every mobile phone user in the UAE must re-register SIM card,” The National, June 28, 2012, http://bit.ly/1k7eFoY.
144 GC4HR, Hear their Voices: Alarming Times for Human Rights Defenders in the Gulf Region & Neighboring Countries.