

Statement
UPR Pre-session on UAE
Geneva, Apr 3, 2023
Delivered by Access Now

1. Access Now is an international organization that works to defend and extend the digital rights of users at risk around the world. Through representation worldwide, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organization, Access Now routinely engages with the United Nations (U.N.) in support of our mission to extend and defend human rights in the digital age.¹
2. This statement focuses on surveillance and state violation of the right to privacy.

Follow-up from UAE's third cycle

3. During the third UPR cycle, UAE received 260 recommendations, supporting 138 and noting 122. We have noted the absence of recommendations regarding the right to privacy and we hope that some light will be brought, during the fourth UPR cycle, to the topic of surveillance as a tool to undermine human rights such as the right to privacy, freedom of expression and freedom of peaceful assembly.

Legal framework related to the right to privacy

4. First of all, the Emirati Constitution provides in its Article 31 for the freedom of communication by means of post, telegraph or other means of communication and guarantees their confidentiality in accordance with the law.
Despite the constitutional basis for the right to privacy, more safeguards are required to bind the parliament and the government with the principle of legitimacy, necessity and proportionality regarding the restriction of the right to privacy.
5. Moreover, the UAE has not ratified the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), among other international human rights instruments.
6. At the regional level, Article 21 of the Arab Charter on Human Rights² provides that “ I. No one shall be subjected to arbitrary or unlawful interference with regard to his privacy, family, home or correspondence, nor to unlawful attacks on his honor or his reputation.

¹ Access Now, About Us, 2021, available at <https://www.accessnow.org/>. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

² Available online: <http://hrlibrary.umn.edu/instree/loas2005.html?msource=UNWDEC19001&tr=y&auid=3337655>

2. Everyone has the right to the protection of the law against such interference or attacks.”
7. The right to privacy is protected in the major international legal instruments. Communications surveillance interferes with the right to privacy, and therefore should only be executed in strict compliance with international human rights law and under impartial, competent judicial oversight, as articulated by the Human Rights Council³ and the International Principles on the Application of Human Rights to Communications Surveillance.⁴

New developments since the last review

8. Since the last UPR review, UAE has continued to attack individuals in the country by violating the right to privacy through state-sanctioned surveillance.
9. In 2018, Citizen Lab announced in its report that UAE is one of the countries where the use of surveillance tools developed by the Israeli firm NSO Group was detected between August 2016 and August 2018.⁵
Based on The Guardian report, at least 12 journalists were subject to surveillance.⁶
The use of Pegasus spyware has negatively affected journalists and human rights defenders, violating their privacy and putting their private and professional lives and security at risk. Among these HRDs we can mention Loujain al-Hathloul and Ahmed Mansoor.
10. On March 13, 2018, **Loujain al-Hathloul**, a Saudi women human rights activist, was kidnapped in the United Arab Emirates (UAE) while driving on the highway and flown back to Saudi Arabia in a private jet, where she was detained until her release on March 15, 2018. On May 15, 2018, al-Hathloul was re-detained,⁷ and seven days later, transferred to a secret prison in Jeddah, where she was subject to interrogation and torture. A 2019 Reuters investigation revealed that al-Hathloul was targeted in 2017 by a team of U.S. mercenaries who surveilled dissidents on behalf of the UAE under a program called Project Raven,⁸ which categorized her as a national security threat and hacked her iPhone before she was arbitrarily detained in the UAE. Evidence suggests that al-Hathloul’s infection with DarkMatter⁹ spyware led to her arbitrary arrest by the UAE’s security services and rendition to Saudi Arabia, where she was detained, imprisoned, and tortured.
11. In August 2016, Citizen Lab findings showed that **Ahmed Mansoor**, a renowned Emirati human rights activist, was targeted with three different surveillance products, including FinFisher’s Finspy spyware in 2011 and Hacking Team’s Remote Control System in 2012. In 2016, he was

³ The Human Rights Council, A/HRC/RES/34/7, The right to privacy in the digital age, available online: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/34/7, April 7, 2017.

⁴ Available online: <https://www.necessaryandproportionate.net>

⁵ Citizen Lab, HIDE AND SEEK Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries, September 18, 2018, available online: <https://citizenlab.ca/2018/09/hidden-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

⁶ The Guardian, FT editor among 180 journalists identified by clients of spyware firm, July 20, 2021, available online: <https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware?fbclid=IwAR1afV5jQIJ15aJb2c4vuOPuTsC4rK6BfblEwxZ9X9xhop6zSi42UAaLbjl>

⁷ See Loujain AlHathloul, <https://www.loujainalhathloul.org/arrest-torture-charges>.

⁸ Reuters, Project Raven, available at: <https://www.reuters.com/investigates/section/usa-raven/>, January 20, 2019

⁹ *Ibid.*

targeted by Pegasus.¹⁰ Project Raven also hacked Mansoor’s device in 2016, and a year later, his wife’s.¹¹ Mansoor was initially jailed for a period of eight months in 2011 after calling for greater political rights and freedoms.¹²

Main recommendations

12. We urge that the right to privacy would be a prominent issue in the upcoming UPR review cycle.

We therefore recommend that UAE:

- a. Amend the Constitution and pass regulations affirming and protecting the human right to privacy;
- b. Cease all surveillance operations and persecution of individuals and respect the right to privacy;
- c. Introduce strong and effective transparency and oversight mechanisms to all matters related to mass surveillance and the acquisition of surveillance technology.

¹⁰ The Citizen Lab, The Million Dollar Dissident, available at: <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>, August 24, 2016

¹¹ Electronic Frontier Foundation, alHathloul Vs DarkMatter, available at: <https://www.eff.org/document/alhathloul-v-darkmatter>, September 12, 2021.

¹² Human Rights Watch, UAE: Free Activists Before Elections, available at: <https://www.hrw.org/news/2011/09/22/uae-free-activists-elections>, September 22, 2011