Access Now submission to the Universal Periodic Review

Israel, Third Cycle

Surveillance technology threatens privacy & free expression

About Access Now

1. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world, including engagement with stakeholders and policymakers in India, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights online. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
2. Access Now advocates an approach to digital security that promotes transparent and accountable policies that protect human rights, including privacy and freedom of expression. Access Now maintains an office in the Middle East and North Africa region to advance protection of digital rights.
3. Access Now draws attention to several urgent threats to human rights and the open internet in Israel, including invasive surveillance and unlawful invasions of privacy.

Domestic and international human rights obligations

4. This is the third review for Israel, last reviewed in 2013, under the Universal Periodic Review mechanism (UPR).
5. Israel has ratified various international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR), the Convention against Torture (CAT), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW).

Developments of digital rights in UAE

6. Israeli companies produce surveillance technology that governments around the world deploy to unlawfully interfere with the privacy and chill the freedom of expression of human rights defenders, peaceful activists, journalists, and political figures targeted for the exercise of their rights.
7. For example, the UAE is currently detaining human rights advocate Ahmed Mansoor.[1] UN experts label his detention a "direct attack on the legitimate work of human rights

[1] BBC, UN experts call for release of UAE activist Ahmed Mansoor, 28 March 2017, <http://www.bbc.com/news/world-middle-east-39416734>.

defenders in the UAE."[2] Mansoor was arrested in 2011, released in less than a year without receiving back his passport being held by authorities, and was jailed again on March 20, 2017. Just before his recent detention, Mansoor worked with civil society to show how he was targeted by expensive tools exploiting unknown vulnerabilities in common smart phones.[3] Researchers showed how an adversary attempted to use sophisticated spyware, sold by the Israel-based NSO Group, to access his private data and communications and track his activities.[4]

8. Researcher Bill Marczak was "able to trace the spyware back to the Royal Group, a conglomerate run by a member of the Al Nahyan family, one of the six ruling families of the Emirates."[5] Following their research into the surveillance of Mansoor and his phone, experts found that, in combination with "prior known targeting of Mansoor by the UAE government," indicators "point to the UAE government as the likely operator behind the targeting."[6]
9. Likewise, on July 11, 2017, an investigation by the Citizen Lab at the University of Toronto's Munk School of Global Affairs and the New York Times revealed evidence that Dr. Simon Barquera, researcher at Mexico's Public Health National Institute, Alejandro Calvillo, Director at El Poder del Consumidor, and Luis Manuel Encarnación, Coordinator of ContraPESO Coalition received targeted attacks with the objective of infecting their mobile devices with surveillance malware exclusively sold to governments by the company NSO Group.[7]
10. According to the evidence, the attacks are related to the target's activities in defense of public health, particularly advocating for a soda-tax and criticizing deficient food labeling regulation.
11. The Pegasus malware commercialized by the NSO Group is used against researchers and civil society organizations. This type of surveillance malware exploits unknown security vulnerabilities (zero-day) in commercial software and products to obtain an

---

[2] OHCHR, UN rights experts urge UAE: "Immediately release Human Rights Defender Ahmed Mansoor", 28 March 2017, <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21449&LangID=E>.

[3] See reporting on Ahmed Mansoor and the purchase, development, and use of spyware by UAE to target and track activists, by Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," The New York Times, 29 May 2016, <https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html>; and Nicole Perlroth, "IPhone Users Urged to Update Software After Security Flaws Are Found," The New York Times, 25 Aug. 2016, <https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html>.

[4] Citizen Lab, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," 24 Aug. 2016, *available at* <https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae>.

[5] Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," The New York Times, 29 May 2016, <https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html>

[6] Citizen Lab, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," 24 Aug. 2016, *available at* <https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae>.

[7] Citizen Lab, "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links," 11 February 2017, https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware.

absolute control of a device, severely compromises the right to privacy, especially when there is no legal controls or democratic oversight of state surveillance.[8] Privacy advocates decry the use of third party malware and surveillance technology, and call for restrictions on its sale, transshipment, procurement, installation, and use.

Right to Privacy

12. The right to privacy is protected in the major international legal instruments Israel has ratified. 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 Council[9] and the International Principles on the Application of Human Rights to Communications Surveillance.[10]
13. The above cases show inadequate oversight of the human rights-infringing activity of Israeli surveillance companies. Based on available evidence, the surveillance enabled by NSO Group's products does not comply with international human rights law respecting the right to privacy.
14. Additionally, under the UN Guiding Principles on Business & Human Rights, governments have the responsibility to protect against business-related human rights abuses by businesses under their power or jurisdiction.

Recommendations

15. Israel can improve its human rights record and treatment of digital rights in several areas. We accordingly recommend that the government of Israel:
    a. Publicly disclose any procurement of or contracts to purchase, maintain, develop, install, service, or operate surveillance technology;
    b. Ensure use of surveillance technology produced or sold by Israeli companies is only used when it is necessary and proportionate to a legitimate aim, subject to meaningful oversight, and only authorized via warrant by an independent, impartial, and competent judicial authority, upon a finding of legality, necessity, and proportionality;[11]
    c. Improve cooperation with United Nations treaty mechanisms and issue standing invitations to UN special procedures such as the UN special rapporteurs on the rights to freedom of expression and opinion, the right to and privacy.
    d. The UPR is an important U.N. process aimed at addressing human rights issues all across the globe. It is a rare mechanism through which citizens around the world get to

---

[8] Access Now, "International groups reject Mexican government surveillance of public health advocates," 16 Feb. 2017, https://www.accessnow.org/international-groups-reject-mexican-government-surveillance-public-health-advocates.

[9] See, e.g., A/HRC/RES/34/7, "The right to privacy in the digital age," 7 April 2017, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/34/7>.

[10] See https://www.necessaryandproportionate.net

[11] Requirements for communications surveillance to satisfy international human rights law are described in the International Principles on the Application of Human Rights to Communications Surveillance (https://necessaryandproportionate.org/principles)

work with governments to improve human rights and hold them accountable to international law. Access Now is grateful to make this submission.

9. For additional information, please contact Access Now General Counsel Peter Micek (peter@accessnow.org).