

Access Now submission to the United Nations Human Rights Council, on the Universal Periodic Review 2018 Cycle for Yemen

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, 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. 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 user rights, including privacy and freedom of expression. Access Now has worked extensively on digital rights including on free expression and web blocking, regulation of Net Neutrality, and data protection.

Domestic and international human rights obligations

3. As outlined in the 2016 Report of the UN High Commissioner for Human Rights on Yemen, Yemen is a party to seven of the nine core international human rights treaties. This includes the International Covenant on Economic, Social, and Cultural Rights (ICCPR) as well as the International Covenant on Civil and Political Rights (ICESCR). It is also a party to the Optional Protocols to the Convention on the Rights of the Child on the involvement of children in armed conflict and on the sale of children, child prostitution, and child pornography.
4. In Article 42 of the Constitution of the Republic of Yemen, it is outlined that the state guarantees freedom of thought and expression in speech, writing, and photography, although it qualifies this statement saying as long as it is “within the limits of the law.”
5. Article 53 of the Constitution of the Republic of Yemen outlines the freedom and confidentiality of mail, telephone, telegram, and all other means of communication, none of which may be “censored, searched, exposed, delayed, or confiscated” except in cases “specified by law and according to a court order.”

Developments of digital rights in Yemen

6. Yemen has been embroiled in a war between the Houthi rebel forces and a Saudi Arabia-led coalition. In September 2014, Houthi forces took control of Yemen's capital, Sana'a, and in March 2015, the coalition attacked Houthi forces. As of November 2017, at least 5,295 civilians had been killed and 8,873 wounded. This war has resulted in many infractions on human rights, digital rights included.
7. Due to the ongoing war, legislation regarding digital rights and internet governance has not been proposed recently. The capitol, and effectively the government, has been controlled by the Houthi group since their takeover in 2015, meaning that they control internet services as well. There are fears that the Saudi-supported forces opposing the Houthis may attempt to target the Ministry of Communications facilities, or that the Houthis will continue to shut down internet access to prevent pro-Hadi groups from using it. Given the instability around the internet and digital realm, little attention is being paid to digital rights. For example, those advocating for a national Internet Governance Forum are being suppressed by the restrictions of wartime.¹
8. Yemen engages in internet shutdowns and related censorship. Measures amounting to internet service disruption, website blocking, and online "kill switches" or "shutdowns" have been widely condemned by international, regional and domestic courts and human rights bodies.
9. UN General Assembly adopted by consensus the resolution, "The safety of journalists and the issue of impunity", which contains an operative paragraph on shutdowns, reading: "*Condemns unequivocally* measures in violation of international human rights law aiming to or that intentionally prevent or disrupt access to or dissemination of information online and offline, aiming to undermine the work of journalists in informing the public, and calls upon all States to cease and refrain from these measures, which cause irreparable harm to efforts at building inclusive and peaceful knowledge societies and democracies."²

Violations of access to information & freedom of expression

10. In December of 2017, the Houthis, the group in control of much of Sana'a since 2015, shut down the internet for about 30 minutes.³ This shutdown came after measures to disrupt and limit access to the internet earlier in the week. This is not the first time the Houthi-controlled Ministry of Communications has shut down the internet. In April of 2015, shortly after the Houthis took over the ministry, they temporarily shut down the internet in Aden

¹ Walid Al-Saqar, "Prospects of a National IGF in Time of War," (Global Information Watch, 2017) https://www.giswatch.org/sites/default/files/gw2017_yemen.pdf

² UN General Assembly, *The safety of journalists and the issue of impunity*, UN Doc. A/C.3/72/L.35/Rev.1 (2017).

³ Grant Baker, "Internet Shutdown in Yemen: Recurring Disruptions Threaten Civilian Safety, Human Rights, and Press Freedom" (SMEX, December 8 2017). <https://smex.org/internet-shutdown-in-yemen-recurring-disruptions-threaten-civilian-safety-human-rights-and-press-freedom/>

following fighting between supporters of president Hadi and Houthi rebels. It is believed that these shutdowns are connected to attempts to cover up atrocities and crimes.

11. Before the shutdown, the Houthis had also been throttling internet speeds across the country, as shown by [many complaints](#) online that the internet was very slow. YemenNet, the Ministry of Communications-controlled ISP (the sole ISP in the country), regularly throttles the internet, according to Walid al-Saqaf, co-founder and chairman of ISOC-Yemen.⁴
12. Prior to the shutdown, popular social media platforms and communication tools such as Facebook, Telegram, Twitter, and WhatsApp were blocked.⁵ These sites are essential to the ability of Yemeni people to access information and connect with each other, especially as families seek to communicate and account for each others' safety in the wake of violence from the war. Many users said they could only access these sites by using a Virtual Private Network (VPN), but through throttling and blocking pages, the Ministry of Communications made it extremely difficult for users to download VPNs.
13. In October of 2017, the Ministry of Communications outlawed the unlicensed practice of online journalism.⁶ This not only hinders reporting and the sharing of information about the ongoing war by local journalists, but restricts Yemeni activists from publishing content on public social media pages. This law comes amidst many Houthi attacks on journalists, such the firing of rocket-propelled grenades at Saleh-aligned television channel Yemen Today and the detention of 41 journalists and media workers.⁷ According to an activist in Sana'a in 2016, anyone caught with digital content on their mobile phone, tablet, or laptop criticising the Houthis risks extrajudicial actions ranging from kidnapping to even assassination.⁸

Violations of the right to privacy

14. Yemen has no laws or regulations protecting the digital privacy of citizens, so cases where private information was published online have emerged.
15. Since the government has a monopoly over the ISP sector, there is a lack of transparency and accountability related to the data transferred through or stored on local servers. According to

⁴ Grant Baker, "Internet Shutdown in Yemen: Recurring Disruptions Threaten Civilian Safety, Human Rights, and Press Freedom" (SMEX, December 8 2017).

⁵ "Houthis limit social media access in Yemen," (AlArabiya.net, December 7 2017), <https://english.alarabiya.net/en/News/middle-east/2017/12/07/Houthis-limit-social-media-access-in-Yemen.html>. Amr Mostafa, "WhatsApp Reportedly Blocked in Yemen, Mobile Operator Cites 'Technical Issues,'" (Global Voices advox, October 9 2016) <https://advox.globalvoices.org/2016/10/10/whatsapp-reportedly-blocked-in-yemen-mobile-operator-cites-technical-issues/>.

"Houthis prohibit social networks in Yemen to obscure the events in Sanaa," (yemen-press.com, December 3 2017) <https://yemen-press.com/news/101858.html>.

⁶ "Yemen: Houthis prohibit publishing on the internet without permission from them," (translated from Arabic) (Al-Quds Al-Arabi, October 21, 2017) <http://www.alquds.co.uk/?p=812691>

⁷ "Houthis holding 41 journalists hostage inside Yemeni TV station," (Reporters Without Borders, December 7 2017) <https://rsf.org/en/news/houthis-holding-41-journalists-hostage-inside-yemeni-tv-station>

⁸ Walid Al-Saqaf, "How the internet is giving Yemen a chance in its darkest hour," (Global Information Society Watch, 2016) <https://www.giswatch.org/sites/default/files/gw2016-yemen.pdf>

an anonymous source found by Walid Al-Saqaf, the national security has backdoor direct access to the servers of YemenNet, exposing sensitive and personal data of millions of Yemeni users.⁹

16. An app called Yemen Phone was made that allowed anyone to access millions of Yemeni citizens' names, phone numbers, and physical addresses. This violation of privacy was not investigated by the government.
17. In 2013, the Supreme Commission for Elections and Referendum made the databases of citizens who applied to work in voter registration positions public. This included their name, data and place of birth, academic qualifications, place of work, addresses, telephone numbers, email addresses, and even their national identity card numbers. They eventually removed telephone numbers and email addresses, while all other information remains accessible on the Commission's official website.

Recommendations

18. The internet enables essential human rights, such as freedom of expression and access to information. Internet shutdowns, or intentional disruptions of access to the internet or mobile networks, applications, and services, are therefore a direct violation of such rights. Access Now recommends that the Yemeni government cease internet shutdowns and pledge to protect the right to freedom of expression online as offline.
19. Due to reports of throttling and slowing internet speeds, Access Now also recommends that the government pass legislation protecting net neutrality. Net neutrality is the principle that internet access should be offered to everyone on a nondiscriminatory basis, without favoring certain websites, applications, or services.
20. The government should not block social media and communications applications, such as Facebook and WhatsApp. These apps are essential to modern communication in the public, and are necessary tools to ensure safety during times of warfare and violence. Means of communication are protected in the Constitution of Yemen, and Access Now requests that the government upholds this law.
21. The Yemeni Government should protect the freedom of speech and expression of opinion, even if it is critical of the government. The government should protect journalists, and prevent and cease all attacks on journalists. Yemen should also repeal the law that bans unlicensed online journalism, as this infringes on freedom of expression, and implies that only those given a license, and therefore in the favor of the government, will be able to report the news.
22. Yemen should pass data protection legislation, protecting users' data from both public and private organizations. The government should also restrict unnecessary collection of data. Access Now recommends public and private sector entities to abide by the principles of security, data protection and privacy by design.

⁹ Walid Al-Saqaf, "A Country in Transition with Its Share of Cyber Challenges," (Global Information Society Watch, 2014) https://www.giswatch.org/sites/default/files/a_country_in_transition_with_its_share_of_cyber_challenges.pdf

23. Governments should not seek to undermine encryption, for instance through backdoors or weakened standards. Encryption remains a security solution and while proposal to undermine this technology continues to flourish, there is no such thing as creating vulnerabilities of backdoor “just for the good guys”. Any policy mandating backdoors into encrypted products would likely be effective for only a minimal time, would be substantially costly, and might harm security in general.¹⁰
24. 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 work with governments to improve human rights and hold them accountable to international law. Access Now is grateful to make this submission.
25. For additional information, please contact Access Now staff Peter Micek (peter@accessnow.org).

¹⁰ “Encryption in the U.S.: Crypto Colloquium Outcomes Report,” (Access Now, January 2018) <https://www.accessnow.org/cms/assets/uploads/2018/02/Encryption-in-the-United-States-Crypto-Colloquium-Outcomes-Report.pdf>