accessnow

How journalists and human rights defenders are targeted online

A detailed report on the Middle East and North Africa

About Access Now

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Founded in 2009, and operating in six continents, Access Now aims to ensure the incremental development and effective implementation of international human rights in the digital era, working on freedom of expression, opinion, and thought, Net Neutrality, privacy and the protection of personal data, digital security, and business and human rights.

Contents

Introduction

You might be targeted as an individual, association, or organization because you take up a cause, embrace a thought, or adopt an opinion that decision makers oppose, or even simply because you defend human rights and reject the policies that violate them. In the previous decade, the Middle East and North Africa region[1] witnessed government actions and practices that hurt human rights, including the collection of activists' personal data, stringent online surveillance, defamation campaigns targeting activists, and the enactment of broad and vague legislation that makes charging and prosecuting activists easier. This report highlights the methods authorities in MENA use to target human rights defenders (HRDs) online for the purpose of infiltration and surveillance. Further, it provides an overview of policies leveraged against activists and HRDs.

As the internet has become embedded in societies across the MENA region over the last decade, our digital hobbies, such as using social media, have become routines and now form an integral component of our daily reality. Due to the way technology has developed, we might easily post or disclose our personal data, putting us at different levels of risk, from making us the target of campaigns that impact the democratic process in elections, to exposing us to criminal attacks such as identity theft.

Access Now works to advance policy and processes to make digital rights protections and security a top priority, for human rights defenders and all internet users. In this context, we have documented concrete examples of cyber threats and blackmail online in the MENA region, in addition to providing information about real cases of digital rights violations and online attacks that groups of individuals have experienced between 2017 and 2018.

Moreover, this report highlights a range of common mistakes we make every day on the internet, which can put our data at risk of "phishing"[2] or exploitation, such as through hacking digital accounts, spying, or misappropriation of our personal data for other purposes. Access Now's Digital Security Helpline[3] has dedicated sections of this report to introduce tips and recommendations to enable you to defend yourself and prevent attacks by using the best possible means for protection, so you can avoid being put at risk or becoming the target of an attack.

1 Hereafter referred to as "MENA."

2 Phishing has been defined as "the fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication." Wikipedia, last accessed 31 May, 2019, URL : https://en.wikipedia.org/wiki/Phishing

3 Methods of targeting HRDs differ based on the country and the laws in force. Consequently, Access Now has a dedicated technical team, the Digital Security Helpline, to help keep you safe online, from protecting your personal data to helping secure your technical infrastructure, websites, and social media accounts. The team provides emergency response and technical assistance across the world on a 24/7 basis, advising civil society organizations, activists, media institutions, journalists, bloggers, and HRDs. Do not hesitate to contact our team at help@accessnow.org. Additional information on the Digital Security Helpline: https://www.accessnow.org/help/

I. How are governments targeting human rights defenders locally?

Activists and HRDs face a panoply of strategies used by government authorities or non-state bad actors to hamper their efforts, especially online, and they are at risk of enhanced surveillance. People who manage civil society organizations and associations that adopt opinions and views that differ from those in power are more susceptible to cyber threats. Cyber threats refer to a set of online attacks perpetrated to harm devices or online networks, or to steal personal data or information that can be used to threaten or blackmail an individual or a group of individuals.

As a result of the large increase in the number of internet users in MENA, which is expected to reach 574 million users[4] in 2019, governments seeking to target human rights activists often turn to social media, as these platforms are full of personal data that we directly or indirectly reveal.

We highlight below the main methods governments use to target individuals online, notably:

1. COLLECTION OF INDIVIDUALS' PERSONAL DATA AND INFORMATION

Personal data has become known as the new "oil" of the digital age, given its potential for exploitation and the impact on our economic, social, or even security situation. The integrity of our personal data and information is connected to a fundamental human right to which every individual across the world is entitled: the right to privacy, which is a cornerstone for building democratic societies. Moreover, in recent years, electronic means have become a crucial tool for communicating with others and exchanging information. This has made governments more interested in the digital sphere and spurred development of their legal and practical ability for control and surveillance in this arena, putting human rights defenders in some MENA countries at heightened risk.

Attackers can more easily gather personal data when individuals, including activists, create accounts on social media sites and provide their personal information without taking any preventive measures to protect their digital data. This disclosure of details about themselves can facilitate phishing. By accessing and analyzing the data contained in the personal accounts on these sites, an attacker can compile a profile of an individual's life, including data that reveal sensitive information such as your health situation, religious and political opinions, organizational relationships, interests, activities, and other data that can make you more prone to targeting, attack, or manipulation.

2. SOCIAL ENGINEERING

There are a number of different ways to conduct surveillance and subsequently target human rights defenders. One of the most common ways is to use so-called social engineering techniques, which have the advantage of being easy to deploy, particularly if an attacker already has general or personal information about the

4 Approximate statistics concerning the number of internet users in MENA in 2019, last visit on 4 March, 2019, URL: https://www.statista.com/statistics/325767/mea-number-of-internet-users

victim. As we have noted, social media sites are considered the primary means to gather such information.

There are numerous examples of the use of social engineering campaigns to attack and manipulate human rights activists. For example, in one Facebook group in Iraq, an attacker claiming to be affiliated with a certain association shared a list of email addresses pertaining to human rights associations and organizations. The attacker then attached a number he claimed to belong to the BBC News channel, inviting all activists on Facebook to send videos of any protests they organize.. In fact, the information was false and the links in the post had nothing to do with what the attacker claimed. This was a way to deceive human rights defenders, spy on them, and interfere with their work, which in this instance was organizing protests in Iraq.

3. SO-CALLED TROLL ARMIES

A "social bot" is a new term that emerged with social media sites. These bots are used in a large number of fake accounts for a specific purpose, such as to defend or attack a certain point of view, in order to influence public opinion or fool targets, forming what is known as "troll armies."[5] There are many examples of the use of social bots[6] in MENA. There are several such cases in Saudi Arabia that illustrate how much traction this form of attack has gained. Following are some examples:

The arrest of women activists in Saudi Arabia

Following the peaceful campaigns conducted by a group of women activists for the purpose of promoting and protecting human rights in Saudi Arabia, the activists have been targeted by the same threats and attempts at blackmail online that they experience offline, further shrinking the space for freely expressing their opinions.

Recently, Saudi authorities issued an official statement announcing that at least six activists[7] are accused of forming a group that allegedly constitutes a threat to state security, for "communicating with foreign parties to undermine the security and stability of the Kingdom of Saudi Arabia and its social fabric" (in Arabic).

Additionally, a campaign using a hashtag that translates to #Agents_to_the_embassies[8] was launched on social media to further smear the image and reputation of these women activists. Pictures showing the activists' faces were published, labelling them as agents and traitors. This information has been widely posted and shared across fictitious accounts managed by Saudi authorities to support their objectives and policies. Furthermore, we at Access Now have observed similar campaigns carried out simultaneously on Twitter, endorsing and encouraging King bin

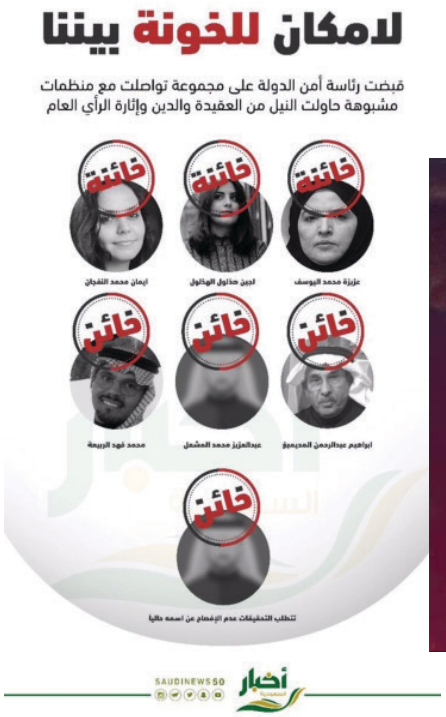
5 How do you solve a problem like troll armies? Access Now, URL: https://www.accessnow.org/solve-problem-like-troll-armies/

6 Report on social bots, Al Jazeera, last visit on 4 March, 2019, URL: https://www.aljazeera.net/programs/newsreports/2017/7/1/%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%B0%D8%A8%D8%A7%D8%A8-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A

7 Saudi women now allowed to drive, but more reforms must follow, Amnesty International, URLhttps://www.amnesty.org/ar/latest/news/2018/06/saudi-arabia-women-now-allowed-to-drive-but-more-reforms-must-follow/

8 "Agents of Embassies... The new Saudi Arabia, either on my side or in prison," Al Jazeera, URL: https://www.aljazeera.net/news/reportsandinterviews/2018/5/19/%D8%B9%D9%85%D9%84%D8%A7%D8%A1-%D8%A7%D9%84%D8%B3%D9%81%D8%A7%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9-%D8%A7%D9%84%D8%AC%D8%AF%D9%8A%D8%AF%D8%A9-%D8%A5%D9%85%D8%A7-%D9%85%D8%B9%D9%8A-%D8%A3%D9%88-%D8%A8%D8%A7%D9%84%D8%B3%D8%AC%D9%86

Salman to detain more activists under the guise of their being "traitors."



Khashoggi case: how did the Saudi regime silence those who discussed the Khashoggi affair online?

With the news breaking about Jamal Khashoggi's murder, in an evident attempt to mute media attention and prevent sharing of information on the story, Saudi Arabia's General Prosecutor[9] issued a reminder that "promoting rumors" and "disseminating fake news" is punishable by law with five years of imprisonment in addition to a fine of up to three million Saudi Riyals (approximately 800,000 USD), in accordance with Article 6 of the Anti-Cybercrime Law[10]. This was an evident attempt to intimidate social media users in general and HRDs in particular, indirectly warning them not to discuss the Khashoggi affair. Despite the case's significance and strong connection to Saudi Arabia, it was absent from Twitter's Trends section in the country, even as it made headlines in global news. According to the "Jadaliyya"[11] website, such methods are considered to be among the most widely used by regimes to silence opposition voices and flood the digital space with supporting messages.

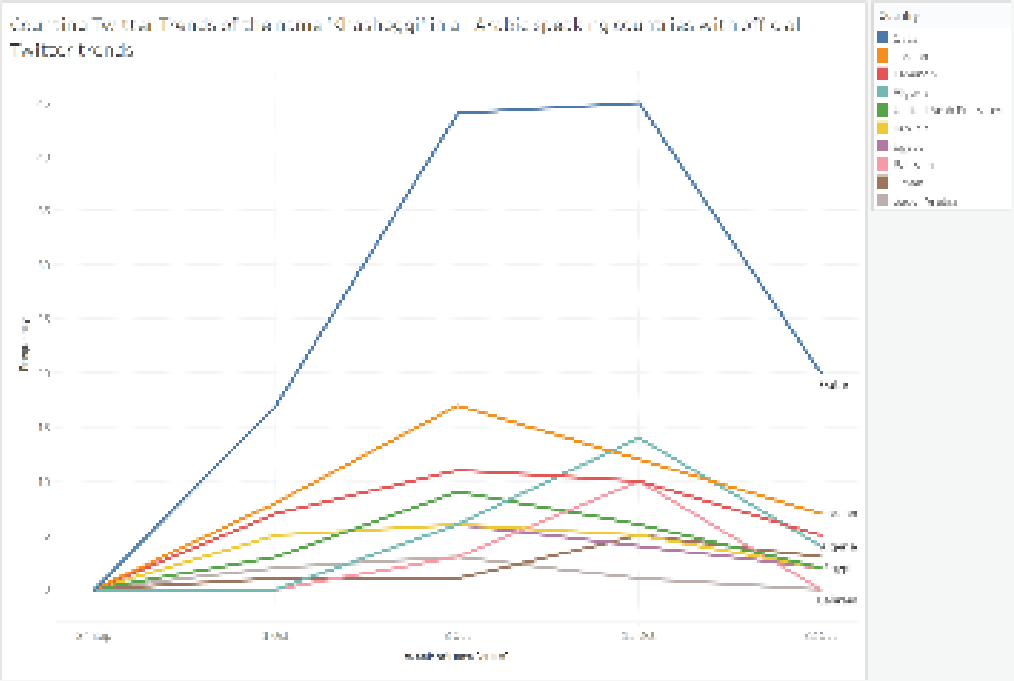
4. DIGITAL SECURITY HELPLINE RECOMMENDATIONS

1. Sharing too much personal information on your social media profile can be

9 Tweet on Makkah Region Emirate's account, General Prosecution in KSA, posted on 13 October, 2018, last visit on 4 March, 2019, URL: https://twitter.com/makkahregion/status/1051162043162738688

10 Anti- Cybercrime law, Royal Decree No. M/17, 26 March, 2017, URL: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf

11 How the Saudi Regime Silences Those Who Discuss the Khashoggi Affair Online, Marc Owen Jones, Jadaliyya, last accessed 4 March 2019 at http://jadaliyya.com/Details/38185



dangerous. Many attackers are able to use trial and error to guess passwords correctly by using sets of commonly shared information (for example, your children's names, your address, birth date, interests, and "likes"). This type of information is often easily found on users' profiles on social networks.

We recommend that you refrain from posting any personal information on these platforms that might put you at risk, such as your address and place of residence, your phone number, your email address, your picture or pictures of your children, information about your schedule, the kind of activities you practice daily, or your routine.

2. It is notable that 50% of the cyber attacks handled by Access Now's Digital Security Helpline in 2018 targeted rights activists' social media or email accounts. Phishing attacks are among the most dangerous techniques used to target human rights activists in MENA.

Therefore, we recommend following these steps to maximize protection of your personal accounts, which also protects your friends and associates:

- Create a complex password that contains letters, numbers, and special characters to reduce the chances of your password being guessed easily.
- Do not trust messages received by email or through social media sites, especially if you do not know the sender. If the message is suspicious, investigate the sender before opening it.
- Access Now's team also recommends the use of a Universal 2nd Factor (U2F), which is a second method to authenticate your password, where you link a key to your computer or smartphone on all your accounts. This prevents an attacker from accessing your account even if your password has been hacked.

II. Policies and techniques states use to silence activists or limit rights and freedoms

1. THE EXPLOITATION OF BROAD AND VAGUE LAWS TO LIMIT THE FREEDOM OF EXPRESSION ONLINE

Internet surveillance takes multiple forms, and in some cases, states use criminal or administrative sanctions to then prosecute individuals because they expressed their opinions online. Authorities legitimize policies for control and ratify legislation for "cybercrime" that can thereafter become a means to silence activists[12]. Over the past few years, many MENA countries have enacted or updated cybercrime laws on the basis of addressing "the rise in online security threats."

Recently, a large number of human rights defenders in MENA have been subject to arrest[13] because they have expressed their opinions on the internet. These defenders are at risk due to the ambiguous and broad terms in cybercrime laws, tailored to favor governments and facilitate the silencing of dissidents and imprisonment of activists.

Notably, authorities across MENA are leveraging accusations of spreading misinformation ("fake news") and are imposing ruthless prison sentences — reaching more than 10 years in some cases — based on what an activist has posted online. These laws are similar to the "state of emergency" laws that are declared in multiple countries, which broadly criminalize poorly defined acts like harming national security, sowing confusion, or inciting violence. Within this framework, Access Now's Digital Security Helpline has registered 261 cases where the digital content published or disseminated on social media was used as the basis for prosecuting those who shared opinions that opposed governments and decision makers in the MENA region in 2017. In 2018, we saw an exponential increase in this rate, with 491 cases.

2. CENSORSHIP OF WEBSITES

Censorship of websites is one of the traditional techniques authorities implement in MENA, used to censor major international news websites, pages dealing with human rights topics, and other websites that authorities deem disruptive and injurious to government-approved values and principles.

In Egypt, for instance, Article 7 of the Anti-Cyber and Information Technology Crimes Law grants authorities a wide array of powers to censor websites if they are suspected to contain information threatening national security,[14] while also failing to clearly define what constitutes a threat to national security. Therefore, this law contributes to expanding government control over online content. As of 2018, the number of blocked websites in Egypt has reached more than 500 sites, including

12 Restricting cybersecurity, violating human rights: cybercrime laws in MENA region, Open Global Rights; Dima Samaro & Wafa Ben Hassine, last accessed on 31 May 2019, URL: https://www.openglobalrights.org/restricting-cybersecurity-violating-human-rights/

13 Free expression in MENA: death by a thousand cuts, Access Now, URL: https://www.accessnow.org/free-expression-in-mena-death-by-a-thousand-cuts/

14 When "cybercrime" laws gag free expression: stopping the dangerous trend across MENA, Access Now, URL: https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/

news sites,[15] the official websites of international human rights organizations, and websites opposing the current ruling power in Egypt.

The Bahraini 2014 Cybercrime Law granted the power of website blocking to multiple governmental organizations, including the Ministry of Interior and the Ministry of Information Affairs. No court order is needed to censor websites that criticize the government, the royal family, or the status quo, or in other ambiguous cases such as the blocking of the Al-Wasat newspaper.[16]

3. TARGETING ELECTRONIC DEVICES BEFORE THEY ARE SOLD

Malware is a type of software installed on electronic devices, such as mobile phones or computers, without the knowledge of the owners. Such software has been designed to achieve specific purposes that serve the interests of the party that wants it installed. Examples of these purposes include surveillance, personal data theft, and other harmful activities.

At times, devices are targeted before the point of sale, with the most popular apps like Facebook, Twitter, and WhatsApp cloned and installed on the device and functioning just like the user expects. These cloned apps look almost identical to the genuine versions, making it extremely difficult to identify them as malware. WhatsApp, a chat app, and Psiphon, a censorship circumvention app, are among the most prominent apps that are cloned to disseminate malware. Attackers — supported by governments and other parties, in most cases — make use of the fact that Google Play is not available in some Arab countries, such as Syria and Sudan, to create cloned apps for malicious purposes and distribute them through informal channels or unreliable platforms.

Activists might be targeted through free apps using APK, or other alternative stores, which some websites offer as as a substitute to the Google Play store. The official Google Store imposes restrictions on the download of some apps and games in certain geographical areas, including Arab countries that are under economic or political sanctions. Yet if you install apps from alternative stores, you might be giving the creators of malware access to your contact list, your network, or your camera.

4. DIGITAL SECURITY HELPLINE RECOMMENDATIONS

We recommend that you avoid using alternative smartphone app stores such as APK to avoid being trapped through use of cloned and malicious apps. When you purchase a new smartphone, we recommend that you uninstall these apps from your phone and reset your device to factory settings before linking it to your personal accounts.

Android: https://support.google.com/android/answer/6088915?hl=ar

iPhone: https://support.apple.com/ar-ae/HT201252

15 Egypt: Almost one year after 500 sites, roughly, have been blocked ahead of the presidential elections, Access Now, URL: https://www.accessnow.org/%D9%85%D8%B5%D8%B1-%D9%85%D8%B1%D8%AA-%D8%B3%D9%86%D8%A9-%D8%AA%D9%82%D8%B1%D9%8A%D8%A8%D8%A7%D9%8B-%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D8%AD%D8%AC%D8%A8-%D9%88%D8%A7%D9%84%D9%85%D9%88%D8%A7%D9%82/

16 Closure of the Al-Wasat newspaper, the only independent newspaper in Bahrain, IFEX, URL: https://www.ifex.org/bahrain/2015/08/07/closure_of_independent_newspaper/ar

III. Other security risks you may confront

1. USING INTERNET (OVER WI-FI) IN PUBLIC PLACES

Coffeeshops, restaurants, hotels, and airports will often offer free Wi-Fi services. Dozens of cities in MENA currently have Wi-Fi in residential and tourist areas, where people can access the internet for free.

With the proliferation of locations offering free Wi-Fi services, it is common to find multiple Wi-Fi options displayed on your mobile device or personal computer. These are the very places where we need to be cautious. The majority of these public networks are either not secure or have shared passwords, and as soon as you log in to one of your accounts, an attacker might be waiting to harm you, as your information is readily available to be stolen. Public Wi-Fi networks are easily hacked using "sniffer" software that intercepts and decodes your data as it is transmitted over a network from your personal computer or smartphone. It is enough for an attacker to be in your general surroundings or to be connected to the same network to be able to achieve this. The attacker can simply log in to the same Wi-Fi network you are using and steal your information using software downloaded from the internet.

Attackers can identify your device and sometimes your name as they access your log in records, as well as the version of the operating system you are using. If you do not have the latest OS update installed on your device, attackers can use any loopholes and bugs to get as much access to your data as possible. Then they can watch what you do online and even get your passwords.

2. DIGITAL SECURITY HELPLINE RECOMMENDATIONS

It is important to use a Virtual Private Network (VPN) when using public Wi-Fi services, especially at airports, hotels, or coffee shops. The only problem is choosing the right VPN. A VPN protects your communications on the public network, but it does not protect your data on the private network you are using. If you are using a commercial VPN, the network operator will be able to see your communications. [17]

We recommend that you review the VPN provider's privacy policy to understand the situations when a provider will hand over your data to the government[18] or law enforcement. In some cases, a government can request that the provider hand over your data without your knowledge, and the law can't protect them.

IV. The role of Access Now and civil society in raising awareness about these threats

Civil society and HRDs have witnessed a number of transformations in recent decades due to technological developments and the growth of the internet in the MENA region.

17 Surveillance Self-Defense Guide, Choosing the VPN That's Right for You, EFF, URL: https://ssd.eff.org/ar/playlist/%D8%B5%D8%AD%D9%81%D9%8A-%D8%AF%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%AA%D8%B1%D8%AD%D8%A7%D9%84%D8%9F#%D8%A7%D8%AE%D8%AA%D9%8A%D8%A7%D8%B1-%D8%B4%D8%A8%D9%83%D8%A9-%D8%AE%D8%A7%D8%B5%D8%A9-%D8%A7%D9%81%D8%AA%D8%B1%D8%A7%D8%B6%D9%8A%D8%A9-%D9%85%D9%84%D8%A7%D8%A6%D9%85%D8%A9-%D9%84%D9%83

18 Ibid. Choosing the VPN That's Right for You, EFF

There have been radical shifts in challenges for defending human rights due to lack of consistency in the law and cross-sectoral requirements and needs, upsetting HRDs' modes of action and putting them in the crosshairs at the same time.

In this context, it is important for civil society organizations to play a strategic role in tackling the human rights challenges of these crises. Based on this understanding, Access Now has prepared advocacy campaigns to help raise awareness about digital rights in MENA. Below are some of the campaigns we have previously conducted, which can help you learn more about online attacks and rights violations.

QUIZ: AM I AT RISK OF GOING TO PRISON IN EGYPT?

Egyptian authorities have a history of escalating attempts to restrict online freedoms, from heavy internet censorship[19] to the Cybercrime Law.[20] They have targeted journalists and civil society activists under the pretext of combating terrorism and achieving stability. Indeed, authorities have arrested a large number of journalists and activists simply for expressing their opinions online.

In collaboration with our partner, the Association of Freedom of Thought and Expression (AFTE),[21] we prepared a quiz to help activists and rights defenders in Egypt understand the daily threats codified by legal texts, and to help convey the voices of those silenced every day, suffering false accusations and trumped-up charges. You can take the quiz to see how everyday online activities might put you at risk of going to prison in Egypt.

THE #KEEPITON CAMPAIGN

The #KeepItOn campaign[22] was launched by Access Now alongside prominent organizations around the world to help those in countries facing internet shutdowns – usually imposed by the government – during specific periods, such as during protests or exams, for the purpose of controlling the flow of information online.

Together the coalition works to keep people connected to the internet and able to exercise their fundamental human rights, including the right to access information and express themselves, whether online or off. Shutdowns represent a blatant violation of fundamental human rights, and at the same time disrupt business and take a heavy economic toll. To support advocacy against them, we are tracking the number of shutdowns globally through the Shutdown Tracker Optimization Service (STOP).[23]

19 Statement opposing Egypt's legalization of website blocking and communications surveillance, Access Now, URL: https://www.accessnow.org/statement-opposing-egypts-legalization-of-website-blocking-and-communications-surveillance-2/

20 United Nations HRC 39: Oral statement on Egypt's cybercrime and media regulation law, Access Now and APC, URL: https://www.accessnow.org/united-nations-hrc-39-oral-statement-on-egypts-cybercrime-and-media-regulation-law/

21 Am I at risk of going to prison in Egypt? Access Now, URL: https://www.accessnow.org/%D9%87%D9%84-%D8%A3%D9%86%D8%A7-%D9%85%D9%8F%D8%B9%D8%B1%D9%91%D9%8E%D8%B6-%D9%84%D8%AE%D8%B7%D8%B1-%D8%A7%D9%84%D8%B0%D9%87%D8%A7%D8%A8-%D8%A5%D9%84%D9%89-%D8%A7%D9%84%D8%B3%D8%AC%D9%86-%D8%A5%D8%B0/

22 #KeepItOn campaign, Access Now, URL:https://www.accessnow.org/keepiton/

23 Launching STOP: the #KeepItOn internet shutdown tracker, Access Now, URL https://www.accessnow.org/keepiton-shutdown-tracker/

For more information:

You can visit our website: www.accessnow.org

Contact us:

Emna Sayadi | MENA campaigner | emna@accessnow.org

Dima Samaro | MENA Policy Associate | dima@accessnow.org

accessnow