Submission to the United Nations Human Rights Council on the Universal Periodic Review, 3rd Cycle, for Egypt

"The Status of Digital Rights in Egypt"

Submitted by Association for Freedom of Thought and Expression (AFTE), Egypt, Access Now and Small Media.

1. AFTE (www.afteegypt.org) is a group of lawyers, researchers and advocates who have been working to support and promote freedom of expression in Egypt since 2007. Our work focuses on a set of priority files: freedom of the press, media, digital rights, freedom of artistic creativity, freedom of information and freedom of expression within Egyptian universities. We rely on four basic strategies: direct legal assistance and strategic litigation, studies and research, monitoring and documenting violations, and advocacy.
2. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation in many countries around the world – including presence in the Middle East and North Africa – 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.

3. Small Media (www.smallmedia.org.uk) Established in 2011, Small Media is a London-based organisation that works to support freedom of expression and access to information globally. We work with our global partners to develop strategies and tools that can support human rights defenders, activists and journalists to work safely and effectively in the digital age. To do this, we provide research, training, and technology support to our network of partners to develop effective, data-driven advocacy strategies and campaigns that can bring about meaningful change.

Commitments to international human rights instruments and mechanisms

4. Egypt has committed to upholding the human rights to privacy and to freedom of opinion and expression, and has ratified many international human rights treaties. Egypt has signed and ratified the International Covenant on Civil and Political Rights ("ICCPR"), the International Covenant on Economic, Social, and Cultural Rights ("ICESCR"), the International Convention on the Elimination of All Forms of Racial Discrimination ("CERD"), and the Convention on the Elimination of All Forms of Discrimination against Women ("CEDAW"), and the African Charter on Human and People's Rights (ACHPR).[1]
5. Article 19 of the ICCPR and Article 9 of the ACHPR explicitly affirm the rights to freedom of expression and freedom of information. As has been observed by the United Nations Human Rights Committee, Article 19(2) of the ICCPR protects both the *form* of

[1] See http://indicators.ohchr.org.

expression adopted by an individual and the *means* they have used for its dissemination – this necessarily includes "electronic and internet-based modes of expression."[2]

6. However, Egypt has not fully participated in the review processes for the ICCPR or the ACHPR. Egypt has not submitted a State report to the Human Rights Committee for the ICCPR since 2002, and has consistently submitted late to the Committee.[3] Egypt is also overdue by six reports to the African Commission on Human and People's Rights.[4] Egypt has also failed to respond to several communications from Special Rapporteur on the freedom of opinion and expression David Kaye, including his request for a country visit in 2015.[5]

7. This review marks the 3rd Cycle for Egypt in the Universal Periodic Review mechanism. In the 2nd Cycle, Egypt received 321 Recommendations, of which Egypt supported 224 recommendations. Of 19 Recommendations on freedom of opinion and expression, Egypt supported 11.[6] Egypt did not receive any Recommendations regarding the right to privacy.

Laws related to privacy, freedom of expression, and communications control

8. Article 57 of the Egyptian Constitution provides for the protection of privacy and the confidentiality of communications and correspondence in Egypt: "The right to privacy may not be violated, shall be protected and may not be infringed upon... Postal, telegraphic and electronic correspondences, telephone calls, and other means of communication are inviolable, and their confidentiality is guaranteed. They may not be confiscated, revealed or monitored except by virtue of a reasoned judicial order, for a definite period, and only in the cases defined by Law." However, there are no laws that review the protection of privacy and confidentiality of personal data and information. Indeed, practices of telecommunications companies and some of their policies towards privacy and terms of contract, and some legal articles, such as: Article II of the law against the crimes of information technology, are contrary to this constitutional provision.

9. The Law on Combating Cybercrimes ("Cybercrime Law") provides new authority for online surveillance, blocking of websites, and monitoring of internet users and the use of communications services in Egypt.[7] Approval of this draft is in line with a series of

---

[2] Human Rights Committee, General Comment 34, available at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[3] See http://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/countries.aspx?CountryCode=EGY&Lang=EN

[4] http://www.achpr.org/states/

[5] See https://freedex.org/resources/reports.

[6] See https://www.upr-info.org/en/review/Egypt/Session-20---October-2014

[7] See "Egyptian Parliament approves Cybercrime Law legalizing blocking of websites and full surveillance of Egyptians", Access Now, available at https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites

rights-harming laws the Parliament has approved since its election in 2015, most notably the Law of Civil Associations, the Law of Institutional Regulation of the Press and Media, and the Protest Law. These laws serve to close space for civil society and deprive citizens of their rights, especially the right to freedom of expression and of association.

10. The Cybercrime Law legalizes broad censorship of the internet and enables executive authorities to block websites, a practice that Egyptian authorities have been employing since 24 May 2017. To date, the number of blocked sites in Egypt has reached at least 500. Article 7 of the Cybercrime Law gives the investigative authority the power to order a website blocked whenever it deems the content to constitute a crime or a threat to security, or a danger to national security or the economy. The investigative authority submits its blocking order to a competent court within 24 hours, and the court issues its decision within a period not exceeding 72 hours, either accepting or rejecting the order. Article 7 effectively legalizes the blocking of websites.

11. The reasons articulated in the Cybercrime Law for blocking websites are vague and broad. For example, the law defines national security as "all that is related to the independence, stability, and security of the homeland and its unity and territorial integrity," and all affairs "related to the Presidency of the Republic, the Defense Council, the National Security Council, the armed forces, military production, the Ministry of Interior, the General Intelligence, the Administrative Oversight Authority, and the organs affiliated with those bodies." Investigative bodies have used these same broad, vague grounds for launching cases against demonstrators and activists (accusing them of calling for demonstrations, publishing crimes, such as in Case 173 against civil society organizations). The failure to clearly define the terms for violating the law means that authorities could misuse or abuse the law to censor what they see as contrary to their policies, justifying censorship as a way to protect national security.

12. Article 2 of the Cybercrime Law regulates the comprehensive monitoring of communications in Egypt, where telecommunications companies are required to retain and store customer usage data for a period of 180 days. These include user-identifiable data, data on the content and substance of the information system, and those relating to the flow of use and the devices used. This means that telecom providers will have data that describes all user practices, such as phone calls and text messages, all data related to them, websites visited, and applications used on smartphones and computers. In addition, the law requires telecommunications companies to comply with any "other data to be determined by a decision" from the NTRA Board of Directors. This means that telecommunication service providers can subsequently be required to collect and retain data not provided for in the law, once an NTRA administrative decision has been issued. The article gives national security authorities the right to access such data, and obligates telecommunications service providers to provide technical facilities of access. The law defines national security agencies as including: "the Presidency, the Armed Forces, the Ministry of the Interior, the General Intelligence and the Administrative Control

-and-full-surveillance-of-egyptians.

Authority." [8]

13. Law No. 10 of 2003 regulates the telecommunications sector in Egypt. The law gives authority to the national security bodies to subject all types of communications to its authority in accordance with Article 67, which states that "the competent authorities of the State shall be subject to the administration of all telecommunication services and networks of any operator or service provider, and to summon operators and maintenance managers of those services and networks in the event of a natural or environmental disaster or in cases where public mobilization is declared in accordance with the provisions of Law No. 87 of 1960 and any other cases related to national security." It is noteworthy that this article was relied upon as a legal provision for cutting communications in Egypt in January 2011. The definition of "national security" in the law is a loose definition that the authorities can use to impose control over the telecommunications sector. [9]

14. Article 64 of Law No. 10 of 2003 obliges all telecommunication service providers to provide "all the technical facilities including systems, programs and communications within the telecommunications network that allow the armed forces and national security bodies to exercise their jurisdiction within the limits of the law. The providers and operators of the telecommunications services and their agents who market these services are obliged to obtain accurate information and data on their users from citizens and from various authorities in the country. "

15. The Emergency Law (No. 162 of 1958) states in article 3 that the President of the Republic is entitled to "monitor messages of any kind and to monitor newspapers, leaflets, publications, editorials, cartoons and all means of expression, publicity and publication before publication, seizure, confiscation and closure of premises." It is noteworthy that this law applies only during the period of declaration by the President of the Republic state of an emergency state, which is the current situation in Egypt, declared since April 2017 and is renewed every three months until now.

16. The Anti-Terrorism Law (No. 94 of 2015) states in article 46 that "the Public Prosecution or the competent investigative authority, as the case may be in a terrorist offense, may authorize a warrant for a period of not more than 30 days to monitor and record the conversations and communications received through Telecommunications and other means of modern communication, recording and photographing what is happening in private places, or through networks, information or websites, and in which they record and control correspondence, regular or electronic messages, publications, parcels and cables of all kinds. The order referred to in the first paragraph of this article may be renewed for a similar period or other periods."

---

[8] New laws.. The thick stick of the state to control the Internet, Association for Freedom of Thought and Expression, 2018

[9] Egypt: Telecommunication Regulation Law, Association for Freedom of Thought and Expression and Article 19 , 2015

17.

Practices of security authorities in monitoring communications

18. According to a decision by the Egyptian Interior Minister of the General Directorate of Information Technology of the Criminal Investigation Department of the Ministry of Interior, a unit called "public follow-up" has been formed. According to the documents of one of the legal investigations conducted with one of the victims, the role of this unit is to monitor and follow up news and information on the web, which may disrupt public peace at present" AFTE has monitored the involvement of this unit in security and judicial pursuits in cases related to freedom of digital expression.

19. In 2013, Egyptian authorities imported ProxySG software from Blue Coat Systems through its agent in Egypt, Systems Engineering of Egypt. This software enables Egyptian authorities to use Deep Packet Inspection technology, which offers great capabilities, including geolocation, tracking, monitoring and filtering The Internet content is collectively unguided and penetrates WattsApp, Webber, Skype and many other programs.[10]

20. In 2014, the Egyptian government, represented by the Ministry of Interior, announced a tender in a limited practice to supply and operate software designed to monitor digital activity on the Internet. The project, was announced by the ministry under the title "Project monitoring the security risks of social networks - the system of measuring public opinion"[11]

21. The tender conditions stipulate that the software required for the Ministry of Interior should be able to monitor and analyze the social networks Facebook, Twitter, YouTube, Instagram, LinkedIn, Webber and WatSab, and the possibility of adding other sites in the future, in addition to the ability of the program to deal with different text files and analysis of the vocabulary contained in them.

22. In the same year, Systems Engineering of Egypt won a contract with the Egyptian Ministry of Interior to monitor social networking sites in Egypt, overtaking other companies such as the British Gamma Group and Israeli Narus. This contract is likely to be the same as the "Security Risk Monitoring Project for Social Networking - Public Opinion Measurement System".[12]

23. In 2014, Vodafone International said in a statement that government agencies in a number of countries where it operates could directly access its network to tap customer calls, including Egypt. Vodafone said it could not provide a complete picture of all the requests it receives because disclosure of this information is illegal in many countries, the same in Egypt.[13]

---

[10] PLANET BLUE COAT - Mapping Global Censorship and Surveillance Tools. CitizenLab, 2013

[11] Administrative court lawsuit to stop social media surveillance, Association for Freedom of Thought and Expression, 2014

[12] Egypt Begins Surveillance Of Facebook, Twitter, And Skype On Unprecedented Scale, Buzz Feed News, 2014

[13] Vodafone admits many governments have direct access to user data, The Verge, 2014.

24. In 2014, French company Ercom supplied the Egyptian authorities with several means of intercepting the connection, called Vortex, in addition to a software that preserves and processes information, called Cortex. Using Vortex and Cortex, Egyptian military intelligence can intercept calls, text messages, control Internet traffic or determine the geographical location of a target.[14]

25. In 2015, Google published a statement that the Egyptian company MCS Holdings - the same company that had previously imported FinFisher software for Egyptian security - has abused the use of SSL / TSL digital certificates technology, one day after they had been acquired; those certificates are used to maintain communication privacy as well as to document identities of communicating parties.[15]

26. MCS Holdings used the digital certificate for a man-in-the-middle attack, an attack that allows it to access packet data as it passes through the network between sender and receiver, including access to user-readable content, as well as their own communications, personal data, impersonation of sites and individuals, and acquisition of confidential data.[16]

27. In 2015, leaked documents from the Italian Hacking Team company revealed that Egyptian authorities had purchased the Remote Control System, a software capable of monitoring the penetration of computers and mobile phones running Windows, Linux, iOS, Android, BlackBerry and Windows Phone.[17]

28. Remote Control System allows surveillance on applications, voice calls, text messages, e-mail messages, camera and microphone use, chat and spy applications on files stored on devices, geolocation and spying on what is written on the keyboard to capture images of the devices and sites being browsed.[18]

29. Leaked documents indicated that the Egyptian company obtained a deal from 2015 to 2017 from Hacking Team for the Ministry of Defense[19]. Later, GNS EGYPT changed its name to INFORT and operates under this name to date.

30. In 2016, attacks were monitored that targeted institutional accounts of Egyptian human rights organizations and personal accounts of human rights defenders. The attacks, based on social engineering, have been used as a major means of targeted fraud by impersonating individuals like Google, Drubox and FedEx to obtain personal data and passwords.[20]

31. In 2017, the UAE purchased the Cerebro software from Amesys - the company later

---

[14] Egypt: a repression made in France, FIDH. 2018
[15] Maintaining digital certificate security, Google Security Blog, 2015
[16] Monitoring communication: Where will the state's attempts to control 'space' lead?, Mada , 2015
[17] Hack of Italian surveillance firm uncovers contract with Egypt, Mada ,2015.
[18] Mapping Hacking Team's "Untraceable" Spyware, CitizenLab, 2014.
[19] The President's Men, Privacy International, 2016.
[20] NILE PHISH- Large-Scale Phishing Campaign Targeting Egyptian Civil Society, Egyptian Initiative for Personal Rights and Citizen lab , 2017

changed its name to Nexa Technologies - and presented it to the Egyptian government. The software enables Egyptian authorities a comprehensive surveillance of communications through the Deep Packet Inspection, including voice calls, text messages, e-mails, instant messages, social networks, and search engine searches.[21]

32. In 2018, technical reports revealed the Egyptian government's use of the Pegasus spy software produced by the Israeli company NSO Group, and the software works through defraud the target person to press a malicious and dedicated link, which once pressed, tries to exploit a series of unknown gaps "zero- day "to penetrate the digital protection features on the phone and download" Pegasus "without the user's knowledge or permission. Once Pegasus is loaded on the phone, it starts dialing C & C to receive and execute operator commands, and sends data to the target person, including private information, passwords, contacts, calendar, text messages, and direct voice calls from applications Mobile Messaging. The operator can even operate the phone camera and microphone to capture and record activity in the surroundings of the phone.[22]

33. In 2018, the use of the Sandvine PacketLogic device was detected, where middle boxes were found to use Deep Packet Inspection technology on one of the Egyptian telecommunications networks. These devices have been used to redirect many users of Internet service providers to digital currency advertisements and scripts.[23]

34. The police in Egypt monitors dating sites, especially for LGBT people. The police tracking of individuals' accounts through applications and dating sites, was reported, with subsequent arresting of individuals by soliciting and agreeing to sex, preparing ambushes for arrest, and monitoring some individuals extracting detailed confessions about sexual history.[24]

35. In 2018, the Supreme Council for Media Regulation, the government body responsible for regulating the media sector in Egypt, formed a committee called "Follow-up Committee for Social Networking Sites", a committee responsible for the daily follow-up of the social networking pages of various social sectors, including youth and adults, as well as in the different social classes, in order to identify daily the changes and developments in the prevailing ideas on these pages.[25]

---

[21] Egypt: a repression made in France, FIDH. 2018
[22] HIDE AND SEEK - Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, Citizen Lab, 2018
[23] BAD TRAFFIC - Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?, Citizen Lab, 2018.
[24] The Trap: Punishing Sexual Difference in Egypt, Egyptian Initiative for Personal Rights,2017
[25] Follow up committee of social networking websites, Supreme Council for Media Regulation.

Egyptian Telecom Companies' privacy policies[26]

36. The communication regulation law, issued in 2003, regulates the communication sector. The national agency for regulation of telecommunication undertakes the management all that relates in communication in Egypt. Egypt has no laws that protect data and personal information.

37. Communication companies and internet service providers require a copy of the ID of its clients. No communication service can be obtained otherwise.

38. Communication companies do not provide clear and detailed information regarding hier privacy policies whether on their website or in communication services they provide to their clients. Some of them do not provide privacy policies at all. While some companies publish a privacy policy on their website, none of those policies comply with the standards for the protection of client data or privacy.

39. Egypt's telecom service providers receive a large amount of personal information, without the existence of mechanisms and obligations from companies to protect and not disclose them. The terms of the contract stipulate that companies may share user data with third parties, whether for law enforcement, marketing or debt collection purposes, without any privacy protection provisions or procedures for data sharing. No companies provide an explanation to users about disclosure procedures.

40. Companies retain data and information collected by customers indefinitely, and there are no procedures that enable users to know or control how they are used.

41. None of the companies provides clarification on the procedures related to securing the data and information of their users.

42. Some service providers in Egypt expressly state in the usage policy that their services may not be used to disseminate content that is incompatible with religions and cultural fabric, to use offensive language to public and political figures, to violate good conduct or to exceed acceptable limits of decency and taste, all of which are terms used by the authorities to limit the freedom of digital expression and to prosecute activists and human rights defenders by security bodies and in courts.

Practices relating to violations of the freedom of digital expression

43. The past four years in Egypt have witnessed violations of the right to freedom of digital expression by Egyptian authorities. AFTE was able to monitor 308 violations; the arrest of citizens based on their digital expression is one of the most widespread violations

[26] Privacy Policies of Communication Companies in Egypt , Association for Freedom of Thought and Expression, 2018.

documented. The Egyptian Ministry of Interior is the number one violator of digital expression in Egypt. Moreover, Egyptian authorities have blocked 512 websites in the last four years, ranging from media and news websites to websites of human rights organizations and websites that provide tools for bypassing internet censorship.

44. The Cybercrime Law legalizes broad censorship of the internet and enables executive authorities to block websites, a practice that Egyptian authorities have been employing since 24 May 2017. To date, the number of blocked sites in Egypt has reached at least 500, and the government recently increased its ability to levy onerous financial penalties on websites.[27]

Recommendations

45. Egypt should review its laws for consistency with its international human rights obligations.

46. Egypt should repeal the Cybercrime Law in full, and not develop any legislation that restricts internet freedom and the freedom of digital expression and privacy.

47. Egypt should repeal Article 19 of the Law of Institutional Regulation of the Press and Media and repeal the articles related to blocking websites in the list of sanctions issued by the Supreme Council for Media Regulation.

48. Egypt should unblock all blocked websites since 2017.

49. Egypt should cease imports of invasive surveillance technology and abolish all security service practices related to the control of communications and the internet.

50. Egypt should halt all interference by security services in the ICT sector, including the control of the communications infrastructure in Egypt.

51. Egypt should amend all articles related to freedom of expression and privacy in the Egyptian Telecommunications Law, in line with international standards for the protection of human rights and in line with the proposals submitted to the government by Egyptian civil society organizations.

52. Egypt should release all prisoners who were arrested and tried on the grounds of expressing their views online.

53. Egypt should obligate telecommunications companies and service providers in Egypt to respect the privacy of their users, and to provide for this under the terms of their contracts, with emphasis on a policy of no exceptions that may lead to any privacy

[27] See “Egypt Can Now Block Websites, Social Media Accounts Deemed a 'Threat'” at https://www.haaretz.com/middle-east-news/egypt/egypt-can-now-block-websites-social-media-accounts-deemed-a-threat-1.7041232.

violations.