PRIVACY INTERNATIONAL

The Right to Privacy in Egypt

Stakeholder Report
Universal Periodic Review
20th Session - Egypt

Submitted by Privacy International, the Egyptian Initiative for Personal Rights, the Association for Freedom of Thought and Expression, and the Association for Progressive Communications

March 2014

Introduction

This stakeholder is a submission by Privacy International (PI), the Egyptian Initiative for Personal Rights (EIPR), the Association for Freedom of Thought and Expression (AFTE), and Association for Progressive Communication (APC). **PI** is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged. **EIPR** is an Egyptian independent rights organization that has worked since 2002 on strengthening and protecting basic rights and freedoms in Egypt, through research, advocacy, and litigation in the fields of civil liberties, economic and social justice, democracy and political rights, and criminal justice. **AFTE** is an independent Association, established in 2006, interested in issues related the protection of freedom of thought and expression. **APC** is an international organization and network with UN's ECOSOC Status. Its mission is to empower and support organizations, social movements and individuals in and through the use of information and communication technologies (ICTs) to build strategic communities and initiatives for the purpose of making meaningful contributions to equitable human development, social justice, participatory political processes and environmental sustainability.

Together PI, EIPR, AFTE and APC wish to bring their concerns about the protection and promotion of the right to privacy in Egypt before the Human Rights Council for consideration in Egypt's upcoming review.

The right to privacy

Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from arbitrary State intervention and from excessive unsolicited intervention by other uninvited individuals.[2] Activities that restrict the right to privacy, such as surveillance and

[1] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[2] Martin Scheinin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 2009, A/HRC/17/34.

censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[3]

As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[4] A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law.[6]

Follow up to the previous UPR

Despite the surveillance regime in place at the time of the last UPR of Egypt on 17th February 2010, there was no mention of the right to privacy and data protection in relations to surveillance, and the resulting violations in the National Report submitted by Egypt in view of its review or in the report of the Working Group. On the other hand, stakeholders raised widespread concerns about the suppression of press freedom, and violence against journalists, and bloggers, as well as online and offline rights in their submissions. The Working Group made several relevant recommendations to the Egyptian government on these issues, including:[7]

- Repeal of articles in the penal code which allow the imprisonment of journalists for their writing and amend the press provisions of the penal code so that they explicitly state that journalists not be imprisoned or otherwise punished for the sole exercise of their right to free expression (Norway) – Recommendation 86
- Take further steps to promote an open and free press where journalists may report on a full spectrum of political, social and economic issues without fear of retribution (Canada) – Recommendation 101;
- Effectively guarantee the exercise of freedom of expression, association and peaceful assembly and the right to participate in public life and politics, in line with the obligations set forth in the Covenant on Civil and Political Rights – Recommendation 102;
- Review its legislation to complete the abolition of imprisonment penalties for publication offences (Netherlands) – Recommendation 103;

[3] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[4] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[5] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

[6] As of December 2013, 101 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

[7] Human Rights Council, *Report of the Working Group on the Universal Periodic Review: Egypt, Fourteenth session, Agenda item 6*, Universal Periodic Review, 26 March 2010, A/HRC/14/17. Available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/125/48/PDF/G1012548.pdf?OpenElement

- Emergency powers should not be abused or used against journalists and bloggers in their exercise of their right to freedom of expression (Ireland) – Recommendation 104;
- Take action to secure that the enjoyment of human rights extends to the Internet, as pronounced by the Human Rights Committee and relevant United Nations resolutions (Sweden) – Recommendation 105.

International obligations related to privacy

Egypt is a signatory to the Universal Declaration of Human Rights ('UDHR') and has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". Article 93 of Egypt's 2014 constitution[8] states:

> *"The state is committed to the agreements, covenants, and international conventions of human rights that were ratified by Egypt. They have the force of law after publication in accordance with the specified circumstances."*

Domestic laws and regulations related to privacy

Article 57 of the **Constitution of Egypt** protects privacy of communications. It states:

> *"Private life is inviolable, safeguarded and may not be infringed upon.*
>
> *Telegraph, postal, and electronic correspondence, telephone calls, and other forms of communication are inviolable, their confidentiality is guaranteed and they may only be confiscated, examined or monitored by causal judicial order, for a limited period of time, and in cases specified by the law.*
>
> *The state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law."*

[8] The 1971 Constitution already upheld this right under Article 45 which reads: *"The law shall protect the inviolability of the private life of citizens. Correspondence, wires, telephone calls and other means of communication shall have their own sanctity and secrecy and may not be confiscated or monitored except by a causal judicial warrant and for a definite period according to the provisions of the law."* And Article 57 which read: "*Any encroachment upon individual freedom or the inviolability of private life of citizens and any other public rights and freedoms guaranteed by the Constitution and the law shall be considered a crime, for which criminal and civil lawsuit shall not be forfeited by prescription. The State shall grant a fair compensation to the victim of such encroachment."* Available at: http://www.sis.gov.eg/En/Templates/Articles/tmpArticles.aspx?CatID=208#.UyHPT1GSw00

Article 58 of the **Constitution of Egypt** safeguards the inviolability of the home:

> *"Homes are inviolable. Except in cases of danger, or if a call for help is made, they may not be entered, searched, monitored or wiretapped except by causal judicial warrant specifying the place, time and purpose thereof. All of the above is to be conducted in cases specified by the law, and in the manner prescribed. Upon entering or searching homes, those inside shall be notified and informed of the warrant issued in this regard."*

Article 113 of the Egyptian Penal Code no. 58/1937 imposes criminal penalties for the unlawful collection of images or recordings for individuals in private places. Also, **Article 309bis** provides for:

> *"a penalty of detention for a period not exceeding one year shall be inflicted on whoever encroaches upon the inviolability of a citizen's private life, by committing one of the following acts in other than the cases legally authorized, or without the consent of the victim:*
>
> *a) Eavesdropping, recording, or transmitting via any instrument whatever its kind, talks having taken place in a special place, or on the telephone.*
> *b) Shooting and taking or transmitting by one of the instruments, whatever its kind, a picture of a person in a private place."*

Article 77 of the Labour Law no. 12/2003 upholds the confidentiality of the employee's file information including punishment and assessment.

Article 97 of the Egyptian Banking Law no. 88/2003 notes the confidentiality of client and account information.
Article 13 of the Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of data on the civil status of citizens.

The **Executive Regulations of Mortgage Finance Law no. 148/2001** issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Ministerial Decree no. 465/2005 has a clause that provides for the confidentiality of the data of clients of mortgage finance companies.

Article 36 (9) of the Mentally Disordered Care Law no. 71/2009 includes a clause on the confidentiality of patient data.

Areas of Concern

1. **<u>Communications surveillance</u>**

In a report presented at the 23rd session Human Rights Council in May 2013, Frank La Rue, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, drew attention to the interrelation between the right to freedom of expression, the

right to privacy and surveillance.[9] The report pointed to the need to further study new modalities of surveillance and recommended the revision of national laws regulating these practices to bring them into line with human rights standards. Mr La Rue's concerns gained particular salience following the leaks made by NSA whistleblower Edward Snowden from June 2013. The right to privacy and its relationship with state surveillance has since been addressed by various UN bodies including the UN General Assembly[10], the Human Rights Council[11] and the High Commissioner for Human Rights[12].

Hosni Mubarak's 30-year regime has left a legacy of problematic state surveillance policies and practices in Egypt. After Mubarak stepped down in February 2011, the Supreme Council of the Armed Forces (SCAF), which took control of the government, maintained communications surveillance practices that originated under Mubarak.[13] The on-going communication surveillance practices outlined in this submission reflect clearly that such practices are still being carried-out by the SCAF, and remain of concern.

a. **Targeted communications surveillance**

The Mubarak regime actively undertook surveillance of protestors during the 25 January 2011 Revolution, with evidence that British technology was sold to the regime and used by its security services. In April 2011, the UK *Guardian* newspaper reported[14] that two Egyptian human rights activists had found documents from surveillance company Gamma International amid hundreds of batons and torture equipment when they broke into the headquarters regime's notorious State Security Investigation services (SII) in March 2011. The documents included an offer, dated 29 June 2010, to provide "FinSpy" software, hardware, installation and training to the SII for 287,000 Euros[15] as well as details of a five-month trial by the Egyptian secret police, which had *"proved to be*

[9] 1 A/HRC/23/40, 17 April 2013. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[10] In November 2013, the Third Committee of the General Assembly approved a resolution titled "Right to Privacy in the Digital Age". The UN General Assembly voted unanimously the resolution on 18 December 2013. In this Resolution, the General Assembly is calling upon Member States to review their procedures, practices and legislation on the surveillance of communications, their interception and collection of personal data, including mass surveillance, with a view to upholding the right to privacy by ensuring the full and effective implementation of all relevant obligations under international human rights law.

[11] The 24th Session of the UN Human Rights Council in September 2013 included a side-event on privacy in the digital age hosted by the governments of Germany, Norway, Austria, Hungary, Liechtenstein and Switzerland during which the International Principles on Application of Human Rights to Communications Surveillance were launched.

[12] In July 2013, following revelations about the operation of the National Security Agency of the United States of America, leaked by Edward Snowden, the High Commissioner for Human Rights, Navi Pillay stated: *"While concerns about national security and criminal activity may justify the exceptional and narrowly-tailored use of surveillance programmes, surveillance without adequate safeguards to protect the right to privacy actually risk impacting negatively on the enjoyment of human rights and fundamental freedoms."*

[13] Reporters Without Borders, *Internet Enemies 2012: Countries under surveillance - Egypt*, 12 March 2012, pp. 42. Available at: https://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf

[14] The Guardian, *British firm offered spying software to Egyptian regime – documents*, 28 April 2011. Available at: http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher

[15] Original documents found documenting the offer and internal discussion within the State Security internal communications about digital spyware and on monitoring SMS were published by the Egyptian Blog for Human Rights on 4 May 2011. Available at: http://ebfhr.blogspot.co.uk/2011/05/state-security-leaks-communicaiton.html

an effective electronic system for penetrating secure systems [which] accesses email boxes of Hotmail, Yahoo and Gmail networks."[16]

'FinSpy' is a product from the FinFisher suite, at the time sold by United Kingdom-based Gamma International. FinFisher comprises a range of malicious software products that infect a computer or mobile device using different techniques; for example, asking a user to download a fake update from what appears to be a legitimate source, such as iTunes, Blackberry or Adobe Flash. Once the user accepts the update, the device (computer, mobile phone, etc.) is infected. Infection allows full access to all the information held on the device. FinFisher products also enable the entity targeting an individual to commandeer and remotely operate microphones and cameras on computers and mobile phones, thus transforming targeted devices into bugs that the individual willingly keeps in close proximity.

In Egypt, some surveillance infrastructure has been provided by Narus, an American company based in California. Narus is a subsidiary of Boeing and has sold surveillance technology to Telecom Egypt, the largest and oldest telecommunications provider in Egypt. Giza systems, an Egyptian consulting firm was in charge of the installation of Narus technology on networks owned by Telecom Egypt.[17] It is unclear as to whether Narus equipment is still in operation currently in Egypt.

Targeted surveillance is still on-going, despite the fall of the Mubarak regime. On 30 January 2014, the Minister of the Interior warned that users of social media, such as Facebook and Twitter could be arrested if they incite violence through their postings. Egyptian authorities claim that they are using modern technology to track those whose posts incite violence against the police or civilians.[18] This worrying development means that the Egyptian government has the technological capacity to carry out surveillance of social media users, to access their accounts and identify potential dissidents, activists, and journalists as well as citizens who are speaking out against the government.

Another recent incident illustrates the culture of impunity for unlawful surveillance, which is still in place in the post-Mubarak-era. In January 2014, Egyptian television station Al-Kahira Wal Nas TV broadcast a series of leaked phone calls featuring the voices of well-known activists, Mohamed Adel and Ahmad Maher, during the January 25 Revolution on its programme called "Black box". Photos of the activists were shown on screen.

Egyptian human rights organisations[19] filed a formal request with the Attorney-General on 31 December 2013, demanding an immediate investigation into the matter.[20] The organisations have

[16] Stephen Grey, *UK firm denies 'cyber-spy' deal with Egypt*, BBC News, 20 September 2011. Available at: http://www.bbc.co.uk/news/technology-14981672

[17] Timothy Karr, *One U.S. Corporation's Role in Egypt's Brutal Crackdown*, Huffington Post, 28 January 2011. Available at: http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html

[18] Ken Hanley, *Egypt expanding social media surveillance targeting opposition*, Digital Journal, 30 January 2014. Available at: http://digitaljournal.com/news/politics/egypt-expanding-social-media-surveillance-targeting-opposition/article/368249

[19] The group of organisations consist of Arab Network for Human Rights Information (ANHRI), Egyptian Initiative for Personal Rights (EIPR), Egyptian Center for Economic and Social Rights (ECESR), Hisham Mubarak Law Center and the Al Haqanya Center.

denounced this leak of private information, arguing that it violates Article 113 of the Egyptian Penal Code no. 58/1937 (see above), which provides, *"violation of privacy including eavesdropping or illegally recording or broadcasting conversation conducted privately or telephonically without the consent of those concerned is an offence punishable by imprisonment."* The organisations have also demanded an investigation into mobile service provider Vodafone, to determine whether it recorded and leak the conversations to the TV station and other parties. Vodafone is known to have previously collaborated in surveillance by the Mubarak regime: in February 2009, it was revealed that the company had handed over communications data to the government to help identify demonstrators who took part in April 2008 protests.[21]

b. Access to communications data

Access to communication data is regulated by the Egyptian Telecommunication Regulation Law, No 10 of 2003[22], which came into force in February 2003. Article 19 requires:

> *"All entities and companies working in the telecommunication field shall provide the NTRA with whatever requested of reports, statistics or information related to its activities except for matters related to National Security."*

Paragraph two of Article 64 of the Telecommunication Regulation Law, No 10 of 2003, reads:

> *"each Operator and Provider shall, at his own expense, provide within the telecommunication networks licensed to him all technical potentials including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law. The provision of the service shall synchronize in time with the availability of required technical potentials. Telecommunication Service Providers and Operators and their marketing agents shall have the right to collect accurate information and data concerning Users from individuals and various entities within the State."*

In light of the extensive powers Article 19 grants the Egyptian General Intelligence Service (EGIS), the Military Intelligence, the Administrative Control Authority, the National Security Investigations Bureau (NSIB), and the Presidency - and the lack of democratic oversight of these agencies - such provisions raise concerns about the level of access state security bodies have to telecommunication networks. In the circumstances, strong safeguards must be in place to ensure the protection of personal data of users, but such safeguards are not known to exist.

---

[20] Egyptian Initiative for Personal Rights, *Egyptian rights organizations demand an immediate investigation into eavesdropping and illegal recordings*, 31 December 2013. Available at: http://eipr.org/en/pressrelease/2013/12/31/1918

[21] Open Net Initiative, *Internet Filtering in Egypt*, 6 August 2012. Available at: https://opennet.net/sites/opennet.net/files/ONI_Egypt_2009.pdf

[22] Available in English at: http://www.tra.gov.eg/uploads/law/law_en.pdf

c. Restrictions on anonymity

Legal restrictions on anonymity and the use of encryption, which are strongly enforced, mean that human rights activists have little or no protection from surveillance, facilitating the government's efforts to monitor and identify them.
Paragraph two of Article 64[23] of the Egyptian Telecommunication Regulation Law, No. 10 of 2003, reads:

> *"Telecommunication Services Operators, Providers, their employees and Users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the NTRA, the Armed Forces and National Security Entities[24], and this shall not apply to encryption equipment of radio and television broadcasting."*

Surveillance is also commonplace in cybercafés, which are a popular means for ordinary Egyptians to communicate on the internet. In February 2005, it was reported that Egypt's Ministry of the Interior ordered Internet café managers to provide access to the personal data of internet users of interest to the Ministry and threatened to close establishments if managers did not comply. In August 2008, this practice developed into a policy whereby the government demanded that Internet café customers must provide their names, e-mail addresses, and phone numbers before being given permission through a coded text message to use the Internet facility.[25]

d. Limiting access to internet and mobile services

Various sources have reported on concerning limitations to access to internet and mobile services, even after the fall of the Mubarak regime.

These include:

- Between 27 January and 2 February 2011 Egyptian authorities disabled Egypt's Border Gateway Protocol Routes, which resulted in all internet traffic being shut down in less than one hour. The authorities then ordered telecommunications companies to cut off all mobile internet and text-messaging services.[26]
- During the demonstrations in November and December 2012, mobile users and activists reported that Voice over Internet Protocol (VoIP) applications and mobile internet access

[23] During the drafting process for the Communications Bill in 2002, the Egyptian Initiative for Personal Rights (EIPR) submitted a memo prepared by its Right to Privacy Program to a group of Members of Parliament (MPs) regarding Article 65 of the Bill, which proposed severe restrictions on the use of encryption techniques. Egyptian Institute for Personal Rights (EIPR), *EIPR Submits Memo on Article 65 of Communications Bill to MPs*, 15 December 2002. Available at: http://eipr.org/en/pressrelease/2002/12/15/253
[24] National Security Entities include: *"All related to the Armed Forces, Military Production, Ministry of Interior and Public Security, National Security Authority, the Presidency and all Authorities related to these entities"*, as defined in Article 1, paragraph 19. [This footnote does not appear in the law proper and has been added as interpretive guidance by the authors of this report]
[25] IFEX, *New Internet café measures tantamount to censorship, says ANHRI*, 11 August 2008. Available at: http://www.ifex.org/egypt/2008/08/11/new_internet_caf_measures_tantamount/
[26] Ripe NCC, *Egypt Network Outage*. Available at: https://stat.ripe.net/events/egypt

more generally were cut off; more widespread connection disruptions were recorded during the protests in March 2013 against President Morsi and the Muslim Brotherhood, although authorities blamed damage to undersea cables in the region for the latter.[27]

e. **Lack of oversight**

Egypt has several intelligence agencies, namely:

1) Al-Mukhabarat al-'Ammah: the General Intelligence and Security Service attached to the Presidency (GIS)

2) Mukhabarat el-Harbeya: the Military Intelligence Service attached to the Ministry of Defence

3) Mabaheth al Amn al Watany: the General Directorate of National Security Investigations under the direct control of the Minister of Interior

4) Hay'at al Riqaba al Idariyya, the Administrative Control Authority, which has the power to tap phone lines according to Telecommunications Act.

These agencies' activities remain very secretive, leaving limited room for oversight and accountability mechanisms and procedures. It was not until 2011 that the name of the GIS director was made public. From its creation, the existence of the GIS was a secret only known to high officials and government newspaper chief editors. Major-General Omar Suleiman, who was the head of the GIS from 1993 to January 2011, was the first GIS head to break this taboo.

Whilst the agencies are given broad powers to carry out surveillance, the Telecommunications Act nonetheless requires a warrant for some surveillance activities; however, this requirement is not practically enforced.

The Egyptian intelligence agencies are failing ensure that their policies and practices adhere to international human rights and adequately protect the rights to privacy and freedom of expression. The different various Egyptian intelligence services, their remit and operations must be reviewed to meet the standards set by *International Principles on the Application of Human Rights to Communications Surveillance.*[28] The State should be transparent about the use and scope of communications surveillance techniques and powers. Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. In addition, the Egyptian authorities should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. The oversight mechanism must be independent of the executive, properly resourced to conduct investigations, and able to command public confidence through regular reporting and public sessions.

---

[27] Freedom House, *Freedom on the Net 2013: Egypt*. Available at: http://www.freedomhouse.org/sites/default/files/resources/FOTN%202013_Egypt.pdf

[28] Launched in September 2013 following a year of consultation, the International Principles on the Application of Human Rights to Communications Surveillance a set of standards that interpret States' human rights obligations in light of new technologies and surveillance capabilities. The Principles are endorsed by 410 civil society organisations around the world, over 40 leading experts, academics and prominent individuals, as well as 4 elected officials. The Principles set for the first time an evaluative framework for assessing surveillance practices in the context of international human rights law. Please refer to the www.necessaryandproportionate.org website for further details.

2. Data protection

Egypt does not have a law regulating the protection of personal data. Privacy is regulated by other provisions as outlined above, including the Penal Code No. 58/1937, the Criminal Procedure Code 150/1950, the Labour Law No. 12/2003, the Banking Law No. 88/2003, and Civil Status Law No. 143/1994, the Executive Regulations of Mortgage Finance Law no. 148/2001, and the Mentally Disordered Care Law no. 71/2009. This is a situation that requires urgent legislative and judicial action in Egypt.

As a consequence, legal regulations regarding privacy-related matters remain scattered and uncoordinated. As Egypt undergoes political and legal reforms towards a democratic state of government accountable to the rule of law, it is essential that issues related to data protection be addressed. The absence of definitions as to what consists personal data and sensitive personal data, the lack of an independent national authority responsible for data protection in Egypt, the lack of requirements for private and public entities to register activities which entail the collection, storage, and sharing of personal data, all raise significant concerns in view of the extensive access given to authorities of users' personal data. In addition, the lack of a data protection authority means there are limited or no opportunities for individuals to seek information on their right to privacy and the protection of their personal data, nor to seek redress, or compensation in case of a violation of these rights. By failing to protect personal data, Egypt is not *"ensur[ing] that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant".*[29]

Given the expansive surveillance policies and practices of the Egyptian authorities outlined throughout this submission, we would urge for the issue of data protection to be addressed and relevant safeguards to be codified. However considering the current instable political context and acknowledging that this is not the adequate time to initiate legal reforms in relations to data protection, it would relevant as a short-term measure for a competent authority (i.e. the High Court) to pronounce itself on the applicability of existing provisions upholding the right to privacy and protecting personal data to extend to the digital domain.

Use of the internet, particularly through mobile phones, has grown significantly in Egypt in recent years; it has become an important tool for mobilising activists, as well as facilitating development activities. Egypt must ensure that existing safeguards protecting privacy and personal data in legal provisions highlighted in previous paragraph, comply with recent interpretations of legal provisions to not distinguish between online and offline rights.

This would confirm recent affirmation by the UN General Assembly (UNGA) Resolution on the right to privacy in the digital age[30] that *"that the same rights that people have offline must also be protected online, including the right to privacy*". The UNGA Resolution called upon Member States to review their procedures, practices and legislation on the surveillance of communications, their

[29] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Article 17), 4 August 1988. Available at: http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument

[30] United Nations General Assembly Resolution, 68/167, *The right to privacy in the digital age*, A/RES/68/167 (18 December 2013). Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

interception and collection of personal data, including mass surveillance, with a view to upholding the right to privacy by ensuring the full and effective implementation of all relevant obligations under international human rights law.

- Registration of mobile telephony users

Article 64 of the Telecommunications Act 10/2003 requires:

> *"Telecommunications Service Providers and Operators and their marketing agents shall collect accurate information and data concerning Users from individuals and various entities within the State"*

Article 65 states that:

> *"The TRA [Telecom Regulation Authority] shall, in cooperation with the Armed Forces and the State concerned entities prepare a prior plan for the operation of Telecommunication Networks to be implemented during natural and environmental disasters and periods of general mobilization according to provisions of Law No. 87 of 1960 regarding general mobilization and any other cases related to National Security. Such plan shall be updated periodically in order to secure Defence and National Security. The Operators and telecommunications Service Providers shall commit themselves to implement such plan."*

Article 67 states that:

> *"The state competent authorities shall have the power to subject to their administration Telecommunications Services and networks of any Operator or Service Provider and call operation and maintenance employees of such services and networks in case of natural or environmental disasters or during declared periods of general mobilization in accordance with the provisions of Law No. 87 of 1960 or any other cases concerning National Security."*

Egypt has a policy of compulsory SIM card registration in place. A TRA policy[31] that came into effect in May 2010 requires that distributors obtain 'the buyer's personal data (as per his ID card) and a copy of his ID card' after verifying the buyer's identity. SIM cards will not be activated until the buyer calls the operator to activate the line (active line) after the Operator's call center verifies the personal data registered in the Operator's database.

Regarding current users, all mobile Operators are required to review the personal data they hold in order to correct, update and complete the data of the current users' lines. This requirement means

[31] National Telecommunications Regulatory Authority, *The New Regulation of the Registration of Consumers' Personal Data in Selling and Activating Mobile Lines*. Available at: http://www.tra.gov.eg/english/News_NewsDetails.asp?PID=39&ID=168

that telecom operators have (at a minimum) read-only access to the civic registry database. Bulk access to the database is not permitted under Article 13 of the civic registry law 143/1994.

SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups. It can have a discriminatory effect by excluding users from accessing mobile networks. It also facilities surveillance and makes tracking and monitoring of users easier for law enforcement authorities.

- Communications monitoring

Articles 19 and 64 of the Telecommunications Act illustrate the overarching powers government authorities have to monitor individuals' communications.

Despite the July 8 Constitutional Declaration[32] and the recently adopted 2014 Constitution, which provides for the privacy of the home, correspondence, telephone calls, and other means of communication, it has been reported that *"security agencies sometimes placed political activists, suspected subversives, journalists, foreigners, and writers under surveillance; screened their correspondence; examined their bank records; searched their persons and their homes; and confiscated personal property. Security services also employed extensive informer systems."*[33]

There are also reports that government authorities have collected, retained and shared the personal data of activists, journalists, human right defenders in breach of existing Egyptian law; such activities have led to identification, arrests, and in some cases prosecutions.[34] If such reports are true, these actions constitute a violation of international standards regarding privacy of communications, and breach Article 57 of the Egyptian Constitution.

Areas of Improvement

Newly adopted constitution

Egypt passed a comprehensively amended version of the 2012 Constitution on 18th January 2014 by referendum.[35] Human rights organisations have expressed reservations about aspects of the

[32] The Interim president had issues a Constitutional Declaration for the transitional period. This declaration upheld the right to privacy under Article 5 and 6. Full text available at: http://www.sis.gov.eg/En/Templates/Articles/tmpArticles.aspx?CatID=2666#.UyHTn1GSw00

[33] See US Department of State, *2013 Human Rights Report: Egypt*. Available at: http://www.state.gov/documents/organization/220562.pdf

[34] Ben Wagner (2012) *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy,* European Parliament, Directorate-General for External Policies, Policy Department, EXPO/B/DROI/2011/28, PE 457.102, pp. 9-10. Available at: http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT(2012)457102_EN.pdf

[35] Full text in English (Unofficial translation) available at: http://www.sis.gov.eg/Newvr/Dustor-en001.pdf

new Constitution[36] particularly in relation its treatment of freedom of expression, freedom of association and the need for rights and freedoms to be interpreted in line with international standards. Nonetheless, we are reassured to see that the new Constitution continues to uphold the right to privacy as a Constitutional right under Articles 57 and 58.[37]

However, the introduction to **Article 31**, concerning information security, is problematic. It reads:

> *"The security of information space is an integral part of the system of national economy and security. The state commits to taking the necessary measures to preserve it in a manner organized by law."*

We are concerned that this provision, which did not appear in the 2012 Constitution, is aimed at creating divergent sets of rights for the online and the offline domains respectively. Such a development would be contrary to the recently adopted UN General Assembly Resolution on privacy in the digital age and directly undermine online users' privacy rights, as well as their fundamental rights to access information, to freedom of expression and opinion.

End of state of emergency

Except for an 18-month period in the early 1980s, Egyptians lived under an official state of emergency from 1967 until 2012. The state of the emergency allowed government authorities to make arrests without warrants and gave security officials the right to search people's homes.

While we welcome the decision to terminate the state of emergency in 2012, we remain concerned about on-going arbitrary restrictions of fundamental rights such as freedom of expression, and information, association, as well as illegal arrests and unlawful searches of homes.[38] Without the extensive powers they had under the state of emergency, the Egyptian authorities must now bring their policies and practices in line with existing protection of human rights upheld in various legislative texts including the new Constitution. The Telecommunications Act, the Anti-Terrorism Act, amongst others, should be amended to reflect Egypt's international human rights obligations.

[36] Article 19, *Legal Analysis: Egypt: Draft Constitution December 2013*, 9 January 2014. Available at: http://www.article19.org/resources.php/resource/37415/en/egypt:-draft-constitution-december-2013#sthash.CefnFj4c.dpuf available at: http://www.article19.org/resources.php/resource/37415/en/egypt:-draft-constitution-december-2013

[37] See above for the text of these provisions.

[38] See reports by: Human Rights Watch, July 2013 http://www.hrw.org/news/2013/07/08/egypt-halt-arbitrary-action-against-brotherhood-media, Front Line Defenders, 5 September 2013, http://www.frontlinedefenders.org/node/23703 and FIDH, November 2013, http://www.fidh.org/en/north-africa-middle-east/egypt/14317-egypt-arrest-of-mr-alaa-abdel-fatah

Recommendations

We recommend that the Egyptian government:

- Ensure that government authorities expand existing protections for the right to privacy and data protection in relevant national laws to ensure the respect of these rights in the context of digital communication;

- Introduce safeguards to ensure that the rights of mobile telephony subscribers in relation to their personal data are guaranteed in accordance with all provisions relating to the protection of personal data;

- Revoke the TRA Regulation of the Registration of Consumers' Personal Data in Selling and Activating Mobile Lines which requires distributors to record the identity of all SIM card users;

- Deregulate the use of strong cryptography to allow online users to communicate anonymously by repelling paragraph two of Article 64 of the Egyptian Telecommunication Regulation Law, No. 10 of 2003 which prohibits the use of encryption technologies without prior consent from the relevant authorities;

- Development accountability mechanisms to oversee its intelligence services, whose work remains highly secretive;

- Investigate claims that illegal communications monitoring is routinely undertaken by the security services and other state authorities; ensure that such practices are ended and responsible individuals held to account if the claims are verified and victims redressed for the violation they experienced;

- Establishes a communications surveillance policy which is in accordance with the *International Principles on the Application of Human Rights to Communications Surveillance*[39] which requires all interference with protected information to be legal, legitimate, necessary, adequate, and proportionate, decided upon by a competent judicial authority, dealt with due process and with the consent of the user amongst others criteria. In addition, an independent oversight mechanism must be set up to ensure transparency and accountability of communications surveillance.

[39] Please refer to the www.necessaryandproportionate.org website for further details.