EGYPT

PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

CONSTITUTION OF EGYPT

Articles 57 and 58 of the Constitution of Egypt explicitly protect the privacy of communications, prohibiting their surveillance except with a reasoned court order for a specific time, in accordance with the law.

THE EGYPTIAN CRIMINAL CODE AND THE CRIMINAL PROCEDURES CODE

According to the Egyptian Criminal Code (Law 58 of 1937) and the Criminal Procedures Code (Law 150 of 1950), a prosecutor or investigative judge may issue a warrant authorizing the interception and recording of individual communications when investigating a possible crime.

Under Article 95 of the Criminal Procedures Code, reasoned warrants from a prosecutor or investigative judge can be issued where they assist in the investigation of any felony or misdemeanor attracting a sentence of over three months, for no more than 30 days and can be renewed once; or by a direct order from an authorized member of the armed forces or security agencies. There are no explicit regulations regarding the latter.

THE COMMUNICATIONS LAW (LAW 10 OF 2003)

The Communications Law (Law 10 of 2003) regulates the communications industry, including law enforcement agencies access to communications and communication infrastructure. It is generally illegal under criminal law to intercept or record private communications except pursuant to a judicial warrant, but the Communications Law allows broad latitude to the armed forces and security agencies to obtain information pursuant to national security concerns, which are not defined.

Article 64 of the Communications Law stipulates that telecom companies must ensure that their communications networks allow the Armed Forces and the various national security agencies to exercise their authorities under the law.

Article 67 of the Communications Law stipulates that all telecommunications operators and providers shall be

There is no directly applicable text in the law, but in accordance with Articles 64 and 67 of the Communications Law, the armed forces and national security agencies have broad latitude to intercept communications with or without an operator's control or oversight.

DISCLOSURE OF COMMUNICATIONS DATA

THE EGYPTIAN CRIMINAL PROCEDURES CODE

The Egyptian Criminal Procedures Code (Law 150 of 1950) gives law enforcement agencies the legal authority to require the disclosure of communications data. Under Article 95 of the Criminal Procedures Code, reasoned warrants from a prosecutor or investigative judge can be issued where they assist in the investigation of any felony or misdemeanour attracting a sentence of over three months, for no more than 30 days and can be renewed once; or the instrument may be a direct order from an authorised member of the armed forces or security agencies. There are no explicit regulations regarding the latter.

NATIONAL SECURITY AND EMERGENCY POWERS

Except as already outlined above, law enforcement agencies and intelligence agencies do not have any other legal authority to invoke special powers in relation to access to communication service providers' customer data and/or network on the grounds of national security or a state of emergency.

OVERSIGHT OF THE USE OF THESE POWERS

Applications made pursuant to the Egyptian Criminal Code and the Criminal Procedures Code require a warrant to be issued by a judge. When making an application to the court, the standard is that the court should be satisfied that the warrant is needed for a 'serious effort' to be made investigating the crime in question.

Anyone claiming violation of privacy or illegal wiretapping can bring a civil suit for damages or file charges for the use of illegal wiretaps, or seek to have illegally obtained evidence dismissed.

Generally, the armed forces and national security agencies are largely exempt from any control or oversight by the communications regulator, the National Telecommunications Regulatory Authority.

CENSORSHIP RELATED POWERS

SHUT-DOWN OF NETWORK AND SERVICES

TELECOMMUNICATIONS REGULATION LAW

Article 67 of the Telecommunications Regulation Law (No. 10 of 2003) provides that all telecommunications

and other major incidents such as natural and environmental disasters or during the declaration of general mobilisation in accordance with the General Mobilisation Law (No. 87 of 1960). In such circumstances, the NTRA, in coordination with the armed forces and the competent authorities, can oblige all telecommunications providers to execute its pre-emptive plan designed for ensuring defence and national security. What constitutes national security is determined by the government. Such control can extend to shutting down a provider's entire network or part of their services.

The NTRA has the power to suspend a telecoms provider's licence if it does not comply with its directions in such circumstances. Telecoms providers have the right to be compensated for damages they suffer as a result of carrying out the plan under Article 68.

BLOCKING OF URLS & IP ADDRESSES

THE CRIMINAL CODE

The Criminal Code contains a number of provisions regarding the dissemination of blasphemous or defamatory material, and may be used to legally require any telecoms provider (including Vodafone) to remove such material insofar as possible.

POWER TO TAKE CONTROL OF VODAFONE'S NETWORK

TELECOMMUNICATIONS REGULATION LAW (NO. 10 OF 2003)

Please refer to 'Shut-down of network and services' above. It is feasible that this legal power could be used by a competent state authority to take control of a network (such as Vodafone's).

OVERSIGHT OF THE USE OF POWERS

TELECOMMUNICATIONS REGULATION LAW NO. 10 OF 2003

Under Article 69, employees assigned by NTRA, the armed forces and national security entities may, upon a resolution by the Minister of Justice in coordination with the minister concerned, be considered judicial officers regarding crimes committed in violation of the Telecommunications Regulation Law (No. 10 of 2003) as related to their positions' scope of work. Otherwise there is no judicial oversight of the NTRA's use of its powers.

This information was originally published in the Legal Annexe to the Vodafone Group Law Enforcement Disclosure Report in June of 2014, which was updated in May of 2017.