BANGLADESH – COUNTRY REPORT

Background

This report outlines the main laws which provide law enforcement and intelligence agencies with legal powers in relation to lawful interception assistance, the disclosure of communications data, certain activities undertaken for reasons of national security or in times of emergency, and censorship of communications under the law of the People's Republic of Bangladesh.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

Section 35 BTRA requires every person establishing or operating a telecommunication system to have a licence. The term, "person" is defined in section 2(24) of the BTRA and includes any natural person, partnership, society, company, corporation, co-operative society or statutory body. In addition, the definitions of "telecommunication", "telecommunication system" and "telecom service" are widely drawn, covering users and service providers in connection with telecommunication services and apparatus.

Section 97(Ka) BTRA (as introduced by the Bangladesh Telecommunications (Amendment) Act 2006) is the sole statutory basis from which the government derives its powers in relation to surveillance and censorship, as outlined below.

Under section 97(Ka) BTRA, on the grounds of national security and public order, the government may empower certain government authorities (intelligence agencies, national security agencies, investigation agencies, or any officer of any law enforcement agency) to suspend or prohibit the transmission of any data or any voice call, and record or collect user information relating to any subscriber to a telecommunications service. This widely drafted provision encompasses interception capabilities. The relevant telecoms operator must provide full support to the authority empowered to use such powers. The BTRA does not provide for any time limits on these powers. As a result, an interception may last for as long as the agency implementing the interception decides.

Under this section, "government" means the Ministry of Home Affairs; provisions under this section are applicable upon approval by the Minister or State Minister of that Ministry.

1.2 Information and Communication Technology Act 2006 (the "ICT Act")

The ICT Act regulates the use of digital signature certificates and the provision of data services and defines a series of offences related to malicious activity online. It provides remedies for offences such as unauthorized damage to computer systems, tampering with computer source code, hacking, publishing false, obscene or defamatory information in electronic form, and publishing false digital signature certificates.

The ICT Controller is an officer appointed under the ICT Act and regulates its implementation. Under section 29 of the ICT Act, the Controller, or any officer authorised by him should investigate any contravention of the ICT Act, or the rules or regulations made under it. In order to do so, the Controller or authorised officer has the same powers as those vested in a Civil Court under Bangladesh's Code of Civil Procedure, which include powers of "discovery and inspection" and "compelling the production of any document".

Under section 30, the ICT Controller may access any computer system, apparatus, data or other material connected with a computer system for the purpose of searching or causing a search to be made for obtaining any information contained in or available to the computer system. The ICT Controller may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

Under section 46 of the ICT Act, if the ICT Controller feels that, in the interests of the sovereignty, integrity, or security of Bangladesh, international relations, public order or for preventing incitement to commission of a legally recognised offence, it is necessary or expedient, they can direct any law enforcement agency of the government to intercept any information transmitted through any computer resource. In

addition, they may order the subscriber or any person in charge of a computer resource to provide all necessary assistance to decrypt the relevant information. The reasons for undertaking such a measure must be recorded in writing.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

There is no direct reference in the BTRA to storage of metadata. In general, storage of data relating to customers is likely to be a condition of a telecommunication operator's individual licence, which commonly requires operators to store metadata for a specified period of time. As billing is done on a monthly basis, operators need to store metadata for subscribers at least for a sufficient period so that the subscribers may make enquiries or seek an itemised bill before payment.

Under the broad powers granted in section 97(Ka) BTRA, on the grounds of national security and public order, the government may require a telecommunications operator to keep records relating to the communications of a specific user. However, when considering whether to make a retention request, the relevant government agency would need to consider the technical resources and capabilities of the operator to retain information.

2.2 Information and Communication Technology Act 2006 (the "ICT Act")

The ICT Controller or any person authorised by him can seek metadata when exercising the investigatory powers provided under section 29 of the ICT Act for the purpose of discovery and inspection, enforcing the attendance of any person and examining him under oath or affirmation, compelling the production of any document, and issuing commissions for the examination of witness for any offence committed under the ICT Act.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

Under section 96 BTRA, the government may, on the grounds of public interest, take possession of any telecommunication system, and any arrangements that are necessary for operating it. It may continue such possession for any time period and keep the operator and his employees engaged on a full-time basis or for a particular time for the purpose of operating such apparatus or system. The government is obliged, however, to pay proper compensation to the owner or the person having control of the radio apparatus or the telecommunication system over which it takes control.

Under section 97 BTRA, when a foreign power declares a state of war, or creates a warlike situation against Bangladesh, when there is an internal rebellion or disorder, or in a situation where the defence or security of Bangladesh or any other urgent state-affair needs to be ensured, the government will have priority over the operator or any other user regarding the use of a telecommunication system.

Moreover, if the President of Bangladesh declares a state of emergency, the government may suspend or amend any licence or certificate or permit issued under the BTRA, or suspend any particular activity of, or a particular service provided by, an operator.

Section 97(Ka) BTRA, as outlined in the sections above, is also applicable in states of emergency or national security.

Furthermore, section 66(Ka) BTRA (incorporated by the Bangladesh Telecommunications (Amendment) Act 2006) empowers the Bangladesh Telecom Regulatory Commission (the "BTRC") to stop any signal, message or request from any subscriber (where it is expedient to do so), in the interest of the sovereignty, integrity, or security of Bangladesh, international relations, public order or for preventing incitement of a legally recognised offence. Operators must assist the BTRC to implement this order.

3.2 Telegraph Act 1885 (the "1885 Act")

It should be noted that some relevant sections of the BTRA's predecessor, the Telegraph Act 1885 (the "1885 Act") are also still in force. However, no operating licences are currently issued under the 1885 Act. As a result the following provisions are no longer used, though we mention them for the sake of completeness:

- Section 5 of the 1885 Act provides that, in the case of a public emergency or in the interest of public safety, the government or any officer authorised by the government, may take temporary possession of any telegraph established, maintained or worked by any person licensed under this Act.
- Under the 1885 Act the government or are authorised officer may order that any message or class of messages to or from any person or class of persons (relating to any particular subject) sent or received by any telegraph, may be blocked, intercepted or detained by, or disclosed to, the government or an officer thereof mentioned in the order.

4. CENSORSHIP

4.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

It should be noted that the national security-related powers granted under s. 97(Ka) BTRA discussed above in section 3.1 could, at least in theory, be used for the purposes of censorship.

4.2 Information and Communication Technology Act 2006 (the "ICT Act")

Under section 45, the ICT Controller (explained above) may issue an order to a licence-holder under the ICT Act to take certain measures or cease certain activities as specified in such order, if necessary to ensure compliance with the provisions of the ICT Act, or rules and regulations made under it.

Under sections 57 and 59 of the ICT Act, if any person deliberately publishes or transmits, or causes to be published or transmitted, on a website or in any electronic form any material which:

1) is false or obscene; or

2) would lead to (or create the possibility of leading to) a deterioration in law and order; or

3) would prejudice the image of the State; or

4) would or may offend religious belief; or

5) incite hostility against any person or organisation,

this activity will be regarded as an offence, and the ICT Controller may make an order to block the communication flow.

5. OVERSIGHT OF THE USE OF POWERS

There are no oversight mechanisms mandated in law in relation to the above legislation. However, the government and the Bangladesh Telecom Regulatory Commission may exercise oversight.

The empowered law enforcement agency may bring a claim against any non-compliance with the rules mentioned above and there are stipulated penalties for first time, second time and third time failures.

6. PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers

There is no direct statutory restriction on publishing aggregated data on government requests for surveillance and censorship powers described above. However the Bangladesh Telecom Regulatory Commission may declare such data to be confidential, exercising its discretion under section 85(1) of the BTRA.

In addition, as the powers are exercised on the grounds of national security and public order, any information relating to the use of such powers is considered confidential information as it may be part of an investigation or used in judicial proceedings. An equivalent position is adopted under the Right to Information Act 2009, under which any information that is given in confidence to any law enforcement agency is excluded from publication under the scope of the Act.

Aggregate data published by government agencies

As far as we are aware, the government does not publish aggregate data relating to its use of the powers described in this report.

7. CYBERSECURITY

7.1 Information & Communication Technology Act, 2006 (the "ICT Act")

As referred to above, under section 46 ICT Act, where the ICT Controller is satisfied that it is necessary in the interest of:

(a) the sovereignty or integrity or security of the state;

(b) friendly relations with foreign states;

(c) public order;

(d) preventing incitement to the commission of any offence punishable under the ICT Act; or

(e) the investigation of any offence

it may, by order, direct any law enforcement agency of the government to intercept, any information transmitted, through any computer resource. This is an exception to the general rule of maintenance of privacy and secrecy of information in Bangladesh that may permit the interception of information in any computer resource. Where the information is such that it ought to be divulged in the public interest, the Controller may require disclosure of such information to law enforcement agencies. This may include information falling into the above categories.

In such circumstances the law enforcement agency appointed by the Controller, can direct a subscriber or any person in charge of a computer resource to extend their facilities to decrypt the information (s.46(2)). This section also provides for interception, monitoring and decryption for the investigation of cybercrimes. The Controller may, by notification in the Official Gazette or Electronic Gazette, declare any computer, computer system or computer network to be a protected system and authorize select law enforcement agencies officials to secure access to the protected systems (s.47).

All matters falling under Section 46 and 47 are dealt with by the Controller by serving notice and the Controller can impose penalties under s. 52 and 53 of the ICT Act.

Under sections 48 to 52, the relevant cybersecurity penalties are as follows:

(a) For failure to furnish document, return and report, a fine of up to 10,000 Taka;

(b) For failure to file a return, information, book etc., a fine of up to 10,000 Taka;

(c) For a failure to maintain books of accounts or record, a fine up to Taka two lakhs;

(d) For a breach of any given instructions, a fine up to 10,000 Taka; and

(e) For contravention of any provision of the ICT Act, a fine of up to 25,000 Taka.

(f) Under the ICT Act, there are eight main cybercrimes (summarised in 7.2 to 7.9 below).

7.2 Damage to a computer, computer system or computer network

Where an individual, without permission of the owner or any person who is in charge of the computer, computer system or computer network in question, carries out one of the following acts, he commits an offence under s. 54 of the ICT Act:

(a) accesses or secures access to a computer, computer system or computer network, for the purpose of destroying information or retrieving or collecting information or assisting another to do so;

(b) downloads, copies or extracts any data, computer database or information from a computer, computer system or computer network, including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or virus into a computer, computer system or computer network;

(d) willingly damages or causes to be damaged in a computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of a computer, computer system or computer network;

(f) denies or causes of the denial of access to any person authorized to access a computer, computer system or computer network by any means;

(g) provides assistance of any kind to facilitate access by another person to a computer, computer system or computer network, in contravention of the provisions of the ICT Act or rules or regulations made thereunder;

(h) for the purpose of advertisement of goods and services, generates or causes the generation of spam or sends unwanted electronic mails without the permission of the originator or subscriber; or

(i) charges the services availed by one person to the account of another by tampering with or manipulating any computer, computer system or computer network.

Should an individual commit any of the crimes described above, their actions are punishable by a fine of up to Taka 1 million (USD12,500) and/or a prison term of 7-14 years.

7.3 Tampering with computer source code

Where a person intentionally or knowingly conceals, destroys or alters (or intentionally or knowingly causes another person to conceal, destroy or alter) any computer source code used for a computer, program, system or network, when the source code in question is required to be kept or maintained by a law in force at that time, they will have committed a cybercrime under s.55.

A breach of Section 55 is punishable by a fine of up to Taka 0.3 million and/or imprisonment for a term of up to three years.

7.4 Hacking with a computer system

Under Section 56, a person is guilty of an offence of hacking if they;

(a) with the intent to cause, or knowing that they are likely to cause, wrongful loss or damage to the public or any person, destroy, delete or alter any information residing in a computer resource or diminish its value or utility or affect it injuriously by any means; or

(b) cause damage through the illegal access to any computer, computer network or any other electronic system which does not belong to them.

Hacking offences are punishable by a fine of up Taka 10 million (USD125,000) and/or a prison term of 7-14 years.

7.5 Punishment for publishing false, obscene or defamatory information in electronic form

According to Section 57, it is an offence to deliberately publish or transmit (or cause to be published or transmitted) on a website or in an electronic form, any material which is false and obscene or where its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all of the relevant circumstances, to read, see or hear the matter contained or embodied within the material. Section 57 also considers hacking to include deliberately publishing or transmitting (or causing to be published or transmitted) any material on a website or in an electronic form, which may undermine law and order, prejudice the image of the state or a person, offend religious belief or incite hostility against any person or organization.

This offence is punishable by a fine of up to Taka 10 million (USD125,000) and/or a prison term of 7-14 years.

7.6 Punishment for unauthorized access to protected systems

Under s.61 it is an offence to secure or attempt to secure access to a 'protected system' as designated by the ICT Controller.

Such an offence is punishable by a fine of up to 1 million Taka (USD12,500) and/or a prison term of 7-14 years.

7.7 Punishment for misrepresentation and obscuring information

Under Section 62, a person making any misrepresentation to, or suppressing any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, commits a criminal offence.

The punishment for misrepresentation and obscuring information is a fine of up to 0.2 million Taka (USD 2,500) and/or a prison term of up to two years.

7.8 Disclosure of confidentiality and privacy

According to Section 63, it is an offence where any person who, in pursuance of any of the powers conferred under the ICT Act or rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material and discloses such material to any other person without the consent of the person concerned.

Where an individual does disclose confidential and private information in breach of this section, he/she will be liable to a fine of up to 0.2 million Taka (USD 2,500) and/or a prison term of up to two years.

7.9 Punishment for publishing false or fraudulent digital signature certificates

Under s. 64 and 65 of the ICT Act, the offence of publishing false or fraudulent digital security certificates is punishable by a fine of up to 0.2 million Taka (USD 2,500) and/or a prison term of up to two years.

Cases relating to the above offences are heard by the Cyber Tribunal of Bangladesh and decisions thereof may be appealed at the Cyber Appellate Tribunal. Under the general judicial regime decisions may also be challenged in the Supreme Court of Bangladesh (ss. 68, 69, 82 and 83 of the ICT Act).

7.10 S.4 of the ICT Act states that if any person commits an offence under the ICT Act from outside Bangladesh using a computer, computer system or computer network located in Bangladesh, the ICT Act will apply as if the entire process of the offence took place in Bangladesh. Furthermore, if any person from within Bangladesh commits an offence under the ICT Act outside of Bangladesh then the Act applies as if the entire process of the offence took place in Bangladesh.

7.10 Upcoming Digital Security Act

The Government is working with a draft Digital Security Act to bring more control over dealings with offences related to cybersecurity. The draft has approval from the Cabinet of Ministers, however, is expected to be further amended and to be placed in the parliament for enactment in late 2017. The Act mandates for the creation of a new Government agency under the act in the name of Digital Security Agency with necessary workforce with a view to fulfilling the purposes of the Digital Security Act.

As per the act there would be a Director General of the Digital Security Agency and the government will appoint additional director general, director, deputy director and assistant direct as well as other officers. If the Director General is pleased that it is expedient and necessary to give directions for the interests of protecting the sovereignty, integrity, security of Bangladesh and friendly relationship of Bangladesh with other countries, public discipline and security, he/she can give directions to law enforcement agencies of the government by order mentioning written reason for obstructing the broadcast of information through any computer resource. The Director General will have the power to:

- take the possession of any computer, computer programme, computer system or computer network or any digital device, digital system or digital network or any programme, information, data which have been stored in any computer or compact disc or removable drive or any other way or access into the same;
- require any person or organization supply the transfer of information or data;
- do whatever is reasonably required for fulfilling the purposes of the act.

In addition, the proposed act declares the following as offences:

- Offences against the Critical Information Infrastructure (punishment: 14 years' imprisonment and / or 10m Taka fine).
- Forgery regarding computer or digital devices (punishment: 5 years' imprisonment and/or 0.3m Taka fine).
- Fraud regarding computers (punishment: 5 years' imprisonment and/or 0.3m Taka fine).
- Non-compliance with the direction of the director general in an emergency (punishment: 5 years' imprisonment and/or 0.3m Taka fine).
- Digital or cyber terrorist activities (punishment: up to life imprisonment and/or 10m Taka fine).
- Violating confidentiality (punishment: 5 years' imprisonment and/or 1m Taka fine).
- Pornography (punishment: 7 years' imprisonment and/or 0.5m Taka fine).
- Defamation, publication of false and obscene material, causing religious offence (punishment: 5 years' imprisonment and/or 0.5m Taka fine).
- Inciting hostility and deterioration of law and order (punishment: 7 years' imprisonment and/or 0.7m Taka fine).

Law stated as at 31 January 2017.