PAKISTAN – 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 Pakistani law.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

1.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA")

Under section 54 of PTRA, the federal government of Pakistan may authorise any person to intercept calls or messages, or to trace calls made through any telecommunications system for national security reasons or for the investigation of any crime. The Pakistan Telecommunication Authority ("PTA") carries out the interceptions as explained in paragraph 1.2 below. Section 54 is generally regarded as providing a very wide scope for the lawful interception of communications under Pakistani law.

Under section 8 of the PTRA the Federal Government may issue legally binding policy directives to the PTA in relation in relation to certain telecommunications matters, including the requirements of national security. Section 8 also grants the Cabinet, or any committee authorised to do so by it, a broadly expressed power to issue policy directives to the PTA, so long as they are not inconsistent with the provisions of the PTRA. The section 8 powers appear to be used to issue directives relating to lawful interception to operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators").

To give one publicly available example, the PTA made a directive on 21 July 2011 prohibiting the use of all encryption mechanisms which conceal communication to the extent that Network Operators cannot monitor it under the Monitoring and Reconciliation of Telephony Traffic Regulations 2010, the scope of which is set out below.

1.2 Monitoring and Reconciliation of Telephony Traffic Regulations 2010 ("MRTT Regulations")

Regulation 4 of the MRTT Regulations sets out mandatory obligations on certain categories of Network Operator to establish systems that enable, among other things, the monitoring of all telecommunication traffic (voice and data) passing through their networks. Regulation 4 makes provision for the Network Operators to comply with these obligations by entering into mutual arrangements with other Network Operators to deploy a collective monitoring system, subject to the approval of the PTA.

Regulation 4(6) sets out more specific requirements for these systems, including that they enable the monitoring, measuring, controlling and recording of traffic in real-time, that they maintain a complete record of all communication signals (including for, but not limited to, billing purposes) and that they maintain a complete list of all Pakistani customers and their details. The monitoring systems must be compatible in order that all this information can be provided to the PTA as required.

Regulation 4(7) states that no person, except the PTA, is allowed to monitor any traffic directly or indirectly on their own or another network without the written permission of the PTA.

Under Regulation 5(8), those Network Operators licensed to operate telecommunications infrastructure, to provide long distance and international telephone services, or to operate local loop (fixed and wireless) and cellular mobile services must provide authorised representatives of the PTA access to obtain information, directly through the system, that relates to any traffic routed through their network, as and when required by the PTA.

The MRTT Regulations gives the PTA legal authority to have real-time access to many Network Operators' networks and services. They do not contain any provisions requiring the PTA to inform the Network Operators that such access has taken place.

1.3 Federal Investigation Agency Act 1974 ("FIAA")

Under section 5 of FIAA, the Federal Investigation Agency ("FIA") has the right to carry out investigations for the purposes of detecting or preventing any crimes under a variety of different laws, including but not limited to those under the Official Secrets Act 1923, the Drugs Act 1976, the Anti-Terrorism Act 1997 (to the extent that the federal government of Pakistan has granted the FIA the authority) and the PTRA. These investigations may require the interception of private communications.

1.4 Investigation for Fair Trial Act 2013 ("IFTA")

Under sections 4-8 of IFTA, certain government agencies may apply to the High Court for a secret warrant permitting the interception or surveillance of any form of digital communication for the purpose of collecting evidence, including the seizure of computing equipment, where the subject of the warrant is suspected of involvement with terrorism-related offences. The agencies in question include the Inter-Services Intelligence, the Intelligence Services of the three branches of the Armed Forces of Pakistan, the Intelligence Bureau and the Police (together the "Intelligence Services").

The scope of IFTA, therefore, is limited to the investigation of terrorism-related offences identified in various laws specified in IFTA, for example the Anti-Terrorism Act 1997 ("Scheduled Offences"). As such the powers of interception that IFTA grants are more limited than those under the PTRA. However, where an intelligence agency wishes to admit evidence to court in the course of a trial on terrorism-related activities related to the Scheduled Offences, it must have obtained a warrant from the court under IFTA.

Before obtaining the warrant, section 16 of IFTA provides that the Intelligence Service must obtain authorisation from the Minister of the Interior. The procedure for obtaining this authorisation is set out in more detail in paragraph 5.2 below. The court warrant is limited in scope to the activities authorised by the Minister of the Interior. The Minister may authorise the use of any technology for the carrying out of interceptions, and may direct Network Operators to implement any technology required to comply with the warrant.

1.5 Prevention of Electronic Crimes Act 2016 ("PECA")

Real-time collection and recording of information

Under section 39 of PECA a duly authorized officer may apply to the Court of competent jurisdiction to collect real time information as well as to collect or record such information in real-time in coordination with the investigation agency. The authorized officer means an officer of the FIA who is duly authorized on behalf of FIA to perform any function of the Investigation Agency, i.e. FIA, under PECA.

The Court may pass orders authorizing the FIA to collect real time information as well as to collect or record such information in real-time in respect of information held by or passing through a service provider provided that the Court has reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation and the duly authorized officer can:

(a) explain why it is believed that the data sought will be available to the person in control of an information system;

(b) identify and explain with specificity the type of information likely to be found on such information system;

(c) identify and explain with specificity the identified offence made out under PECA in respect of which the warrant is sought;

(d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued;

(e) specify what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation;

(f) explain why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and

(g) explain why, to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.

(h) Real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days. Further, notwithstanding anything contained in any law to the contrary, the information collected shall be admissible as evidence in Court. Additionally, the period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period. Finally the Court may also require the designated agency to keep confidential the fact of the execution of any power provided for under section 39 and any information relating to it.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Monitoring and Reconciliation of Telephony Traffic Regulations 2010 (the "MRTT Regulations"), the Federal Investigation Agency Act 1974 ("FIAA") and the Investigation for Fair Trial Act 2013 ("IFTA")

The provisions of the MRTT Regulations, FIAA and IFTA as set out in paragraphs 1.2 to 1.4 above also apply to the collection and disclosure of communications data.

Under the MRTT Regulations, operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators")

must configure their systems to enable the Pakistan Telecommunications Authority ("PTA") to carry out certain activities including but not limited to monitoring, controlling, measuring and recording all traffic over the network in real-time, as set out in paragraph 1.2 above.

2.2 Code of Criminal Procedure 1898, as amended ("CCrP")

Under section 94 of CCrP, a court or a police officer in charge of a police station may order the production of 'any document or other thing' if they consider that it is necessary or desirable for the purposes of the investigation of a crime (subject to limited exceptions). This means that legal persons in Pakistan can be required to produce a wide range of information, which may include data relating to private communications, to the court or to an officer in charge of a police station, under section 94. Refusal to produce the required information can be punished by a fine or a prison sentence, or both.

2.3 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 32 of PECA a service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and subject to the production of a warrant issued by the Court provide that data to the investigation agency or the authorized officer whenever so required.

Violation of this section by a telecommunications service provider or network operator shall be deemed to be a violation of the terms and conditions of its licence and shall be treated as a such under the PTRA.

Note that PECA also contains a number of general powers relating to the acquisition, preservation, search or seizure and inspection of data held on information systems as may be reasonably required for the purposes of a criminal investigation or criminal proceedings. These powers are also subject to the authority of the Court.

3. NATIONAL SECURITY/EMERGENCY POWERS

3.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA")

As stated in paragraph 1.1 above, section 54 of PTRA grants the federal government of Pakistan the power to authorise any person to intercept any form of private communications on the ground of national security, and so the procedure for interception as set out in that Act applies in cases of national security.

Section 54 (3) of PTRA also provides that, in the event that the President of Pakistan declares a national state of emergency, the federal government has the power to modify all licences granted to operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators"), and the federal government can order the immediate suspension of Network Operators' networks or any of their individual services. The government has used section 54 to suspend and shut down services, as well as intercept communications, during periods of national emergency.

Under section 54(2) of PTRA, in a time of war or civil unrest, the federal government of Pakistan has priority use of any telecommunications networks.

Under section 8(2)(c) of the PTRA, the federal government may make specific directives to the Pakistan Telecommunication Authority ("PTA") in relation to the requirements of national security on telecommunications networks.

3.2 Investigation for Fair Trial Act 2013 ("IFTA")

Sections 4-8 of the IFTA, as described in paragraph 1.4 above, also allows interceptions of communications on grounds of national security since it gives powers for preventing terrorism activities that may fall under the Scheduled Offences.

3.3 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 49 of PECA the Federal Government may constitute one or more computer emergency response teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan. A computer emergency response team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed.

4. CENSORSHIP RELATED POWERS

Power to shut down networks or service categories

4.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA") and Pakistan Telecommunication Rules 2000 ("PTR")

Under section 21(4)(f) of the PTRA, all licences granted by the Pakistan Telecommunication Authority ("PTA") to operators of telecommunications networks and providers of telecommunications services ("Network Operators") may, among other things, contain a provision requiring a Network Operator to terminate a telecommunications service provided to a user who has misused the service and continues to misuse it having been informed of such misuse by the Network Operator.

Under section 9 of the PTR, the PTA may monitor compliance by Network Operators with the terms of their licences and their obligations under the PTRA. Once a written notice has been sent to a Network Operator by the PTA alleging any breach of the terms of its licence, the Network Operator has 30 days to demonstrate that the issue has been resolved. If the alleged contravention remains unresolved the PTA may issue an enforcement order, and if the contravention still persists 30 days after the serving of the order, then the PTA may order the termination of the Network Operator's licence.

As set out in paragraph 3.1 above, following the declaration of

a state of emergency by the President of Pakistan, the federal government can suspend any or all licences of Network Operators. Also, as set out in paragraph 3.1 above, the federal government has used s. 54(2) of PTRA to shut down or suspend telecommunications networks or certain services in a time of war or of civil unrest. At present, this latter power is exercised frequently by the federal government to shut down text messaging and other cellular network services in Pakistan.

Blocking of web pages and IP addresses

Under section 31(d) of PTRA, the dissemination of electronic or digital information which is considered false, indecent or obscene is a criminal offence. However, 'false', 'indecent' and 'obscene' are not specifically defined in PTRA.

4.2 Inter-Ministerial Committee for the Evaluation of Websites ("IMCEW") and Pakistani Penal Code 1860, as amended (the "Pakistani Penal Code")

In 2006 the Prime Minister of Pakistan created the IMCEW with a mandate to restrict offensive online content. It consists of representatives from government ministries including the Ministry of the Interior, the PTA, the Cabinet and the security services. Where IMCEW decides that a website or IP address should be blocked, the Pakistani Ministry of Information Technology directs the PTA to perform the blocking.

The term 'offensive' is not specifically defined in Pakistani law in relation to online content. In line with the provisions of the Pakistani Penal Code relating to offensive conduct, it seems likely that online content which is deemed to be offensive will include content that offends a wide range of religious beliefs in Pakistan. This includes (but is not limited to), content that injures or defiles places of worship, content including words that deliberately attempt to wound religious feelings or derogatory remarks in respect of holy people, insults to religion that are intended to incite outrage, and misuse of descriptions or titles of religious groups.

4.3 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 37 of PECA the Authority shall have the power to remove or block or issue directions for removal or blocking of access to any information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under PECA.

4.4 Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communications Regulations 2009, as amended ("SUFOC Regulations")

The SUFOC Regulations provide that Network Operators must have procedures in place, approved by the PTA, to minimise spam emails and any unsolicited, fraudulent and obnoxious communications.

Under regulation 5 of the SUFOC Regulations, all Network Operators must maintain blacklists of those who have made fraudulent communications over their network. Once a customer has been involved in sending a fraudulent communication on more than one occasion, they will be banned from subscribing for any cellular mobile services.

Network Operators must also maintain blacklists of telemarketers who have violated their licence to conduct telemarketing activities under regulation 6 of the SUFOC Regulations. Customers on this blacklist will not be permitted to obtain another licence to conduct telemarketing.

Regulation 10 and Annex C of the SUFOC Regulations also provide that Network Operators must make blacklists and greylists of customers who have made obnoxious communications. These are messages transmitted over the network with the intention to cause harassment or distress. Customers on greylists will have their services restricted, while those on a blacklist will be limited to only making emergency calls on their network.

Unauthorized issuance of SIM cards etc.

4.5 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 17 of PECA states that whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or universal integrated circuit card (UICC) or other portable module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phones or other digital devices such as tablets without obtaining and verification of the subscriber's identity in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

5. OVERSIGHT OF THE USE OF THESE POWERS

5.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA")

Lawful interceptions of private communications under PTRA are not subject to any additional oversight procedures, and nor is there any appeals process for particular individuals who believe that their information has been unfairly collected.

5.2 Investigation for Fair Trial Act 2013 ("IFTA")

To obtain a warrant under IFTA, sections 6-7 provide that the Inter-Services Intelligence, the Intelligence Services of the three branches of the Armed Forces of Pakistan, the Intelligence Bureau or the Police (an "Intelligence Service") must make a report to the Federal Minister of the Interior. The minister will then permit the Intelligence Service in question to go before a judge of the High Court of Pakistan if he deems there to be a reasonable threat that a terrorism offence may be committed, and that an interception of communications would provide evidence of this.

The hearing before a judge must take place in chambers and the authorised officer must personally present the application. Under section 10(b) of IFTA, a warrant will only be granted if the

judge deems there to be a reasonable threat of a terrorist act about which an interception of communications will provide evidence.

The warrant will allow interception activities to take place for up to 60 days, which is renewable on a further application to the court. The Intelligence Service that has received a warrant then approaches the relevant Network Operator directly and they are legally obliged to implement the interception or maintain the surveillance activity (as applicable). The Network Operator has a general duty of co-operation with the relevant Intelligence Service and must ensure confidentiality in relation to the assistance that it gives in relation to the warrant. Network Operators enjoy immunity from prosecution for their activities under IFTA.

The court warrant may authorise any form of surveillance or interception to take place. Therefore, it is possible that the Intelligence Services would be able to access private communications and related data without notification to the Network Operator. Furthermore, as the court hearing takes place in secret, there is no opportunity for the subject of the interception or surveillance to appeal until the evidence is brought before a court in relation to any crime committed.

5.3 Constitution of Pakistan and the Freedom of Information Ordinance 2002 ("FIO")

Article 19-A of the Constitution of Pakistan states that all citizens must have the right to access information in all matters of public importance, subject to reasonable restrictions imposed by the law.

Under the FIO, no citizen will be denied access to records held by public bodies unless disclosure of that information would, among other things, harm relations between Pakistan and other countries, cause an offence to be committed, prejudice an investigation, invade the privacy of any individual other than the requestor, or cause significant damage to the financial interests of any party.

Under section 8 of the FIO, records relating to or connected with the defences forces or defence installations, or are ancillary to defence and national security, are exempt from the records that citizens may request access to under the FIO.

5.4 Prevention of Electronic Crimes Act 2016 ("PECA")

The Federal Investigation Agency (FIA) has been designated as the Investigation Agency under PECA.

6. PUBLICATION OF LAWS AND AGGREGATE DATA RELATING TO LAWFUL INTERCEPT AND COMMUNICATIONS DATA REQUESTS

Publication of laws

6.1 Constitution of Pakistan and the Freedom of Information Ordinance 2002 ("FIO")

As stated in paragraph 5.3 above, all citizens have the right to information held by public authorities that is on the public record, subject to certain restrictions and exemptions. Therefore, unless the information in question falls under one of these restrictions or exemptions, there is no legal authority for the government to prevent the publication of the laws to which operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators") are subject.

Publication of Aggregate Data

6.2 Official Secrets Act 1923 (the "OSA")

Under section 5 of the OSA, it is an offence for any person, who has in his possession or control information which has been entrusted to him in confidence by a public servant, to intentionally communicate such information to anyone who is not authorised to receive it.

Such disclosure of confidential information relating to lawful interceptions and communication data requests, including the aggregate number of them over a defined period of time (assuming that a Network Operator has such information), may constitute an offence under section 5.

6.3 Investigation for Fair Trial Act 2013 ("IFTA")

As stated in paragraph 1.4 above, interceptions made under IFTA are given lawful authority by a secret court process and are implemented by Network Operators operating under a duty of confidentiality. In some circumstances data relating to IFTA interceptions may, when used as evidence at trial, subsequently be included in the official records of the trial at the court in question.

6.4 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 53 of PECA, the FIA shall submit a half yearly report to both houses of the Parliament for consideration by the relevent Committee in camera, in respect of its activities, without disclosing identity information, in a manner as prescribed under PECA.

7. CYBERSECURITY

Pakistan is yet to create specific legislation that imposes obligations on companies to take measures to improve their IT security posture or perform other tasks of a defensive nature, such as to report any material breaches of their IT security to a regulator. The only provisions that are applicable in this regards are those contained within the Prevention of Electronic Crimes Act.

7.1 Prevention of Electronic Crimes Act 2016 ("PECA")

Section 41 PECA which relates to the "confidentiality of information" provides that notwithstanding any immunity granted under any other law for the time being in force, any;

(i) person including a service provider while providing services under the terms of a lawful contract or otherwise in accordance with the law; or

(ii) authorized officer,

who has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract with the intent to cause or knowing that he is likely to cause harm, wrongful loss or gain to any person or compromise the confidentiality of such material or data, shall be punished with imprisonment for a term which may extend to three years or with a fine which may extend to one million rupees or with both.

Note that the burden of proof of any defence put forward by an accused service provider or an authorized officer that he was acting in good faith shall be on the service provider or authorized officer in question.

Moreover, Section 48 PECA which relates to the "prevention of electronic crimes" states that the Federal Government and the Pakistan Telecommunications Authority ("PTA") hold the power to issue directives to be followed by the owners of designated information systems or service providers in the interest of preventing any offence under the PECA. Where an owner of the information system who is not a licensee of the PTA violates any directives issued to it in accordance with Section 48, they shall be guilty of an offence punishable, if committed for the first time, with a fine which may extend to ten million rupees and upon any subsequent conviction with imprisonment which may extend to six months or with a fine or with both. On the other hand, where the violation is committed by a licensee of the PTA, the violation shall be deemed to be a violation of the terms and conditions of the licensee's licence and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act 1996.

According to Section 29(1) the Federal Government has designated the Federal Investigation Agency (the "FIA") as the investigatory agency for the purposes of investigating offences of PECA. Under Section 30, only an authorized officer of the FIA shall have the powers to investigate an offence.

The statutory provisions of the PECA that are regulated by the PTA include;

- Section 32 which concerns the retention of traffic data;
- Section 37 which regulates unlawful online content; and
- Section 48 which concerns the prevention of electronic crimes.

Any decision of the FIA or PTA can be appealed to the special designated courts under Section 47 of the PECA.

8. CYBERCRIME

8.1 Prevention of Electronic Crimes Act 2016 ("PECA")

The PECA also regulates, deals with, and penalises hacking and other forms of unauthorised activity relating to IT networks and systems. These may include commissioning DDoS attacks, inserting malware into IT systems, accessing IT systems using stolen credentials and so on.

The provisions of the PECA explicitly prohibit a wide range of activities, including the following:

Statutory Reference	Offence	Penalty
Section 3	Unauthorized access to an information system or data Described as, with dishonest intent, gaining unauthorized access to any information system or data	Fine which may extend to fifty thousand rupees and/or imprisonment for a term which may extend to three months
Section 4	Unauthorized copying or transmission of data Described as, with dishonest intent and without authorization, copying or otherwise transmitting or causing to be transmitted any data	A fine which may extend to one hundred thousand rupees and/or imprisonment for a term which may extend to six months
Section 5	Interference with an information system or data Described as, with dishonest intent, interfering with, damaging, causing to be interfered with or damaging any part or whole of an information system or data	A fine which may extend to five hundred thousand rupees and/or imprisonment which may extend to two years
Section 6	Unauthorized access to a critical infrastructure information system or data Described as, with dishonest intent, gaining unauthorized access to any critical infrastructure information system or data	A fine which may extend to one million rupees and/or imprisonment which may extend to three years
Section 7	Unauthorized copying or transmission of critical infrastructure data Described as, with dishonest intent, and without authorization copying or otherwise transmitting or causing to be transmitted any critical infrastructure data	A fine which may extend to five million rupees and/or imprisonment for a term which may extend to five years
Section 8	Interference with a critical infrastructure information system or data Described as, with dishonest intent, interfering with, damaging, causing to be interfered with or damaging any part or whole of a critical information system or data	A fine which may extend to ten million rupees and/or imprisonment which may extend to seven years
Section 10	Cyber terrorism Described as committing or threatening to commit any of the offences under Sections 6, 7, 8 or 9, where the commission or threat is with the intent to: (a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance inter-faith, sectarian or ethnic hatred; or (c) advance the objectives of organizations or individuals or groups prescribed under the law	A fine which may extend to fifty million rupees and/or imprisonment of either description for a term which may extend to fourteen years

Statutory Reference	Offence	Penalty
Section 15	Making, obtaining or supplying a device for use in an offence Described as producing, making, generating, adapting, exporting, supplying, offering to supply or importing for use any information system, data or device, with the intent for it to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under the PECA	(Without prejudice to any other liability that he may incur in this regards) a fine which may extend to fifty thousand rupees and/or imprisonment for a term which may extend to six months
Section 17	Unauthorized issuance of SIM cards etc. Described as selling or otherwise providing a subscriber identity module (SIM) card, re-usable identification module (R-IUM) or other portable memory chip designed to be used in cellular mobile or wireless phone for the purposes of transmitting information without obtaining and verifying the subscriber's antecedents in the mode and manner for the time being approved by the Authority	A fine which may extend to five hundred thousand rupees and/or imprisonment for a term which may extend to three years
Section 18	Tampering, etc. of communication equipment Described as unlawfully or without authorization changing, altering, tampering with or re-programing the unique device identifier of any communication equipment including a cellular or wireless handset and starting to use or market such a device for the purposes of transmitting and receiving information Note, a "unique device identifier" is an electronic equipment identifier which is unique to a mobile wireless communication device	A fine which may extend to one million rupees and/or imprisonment which may extend to three years
Section 19	Unauthorized interception Described as, with dishonest intent, committing unauthorized interception by technical means of; (a) any transmission that is not intended to be and is not open to the public, from or within an information system; or (b) electromagnetic emissions from an information system that are carrying data	A fine which may extend to five hundred thousand rupees and/or imprisonment of either description for a term which may extend to two years
Section 23	Malicious code Described as willfully and without authorization writing, offering, making available, distributing or transmitting malicious code through an information system or device, with the intention to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data	A fine which may extend to one million rupees and/or imprisonment for a term which may extend to two years

Statutory Reference	Offence	Penalty
Section 24	Cyber stalking Described as with the intent to coerce, intimidate or harass any person, using an information system, information system network, the Internet, a website, electronic mail or any other similar means of communication to– (a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; (b) monitor the use by a person of the Internet, electronic mail, text message or any other form of electronic communication; (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress in the mind of such person; or (d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person Where the victim of the cyber stalking activity committed is a minor	A fine which may extend to one million rupees and/or imprisonment for a term which may extend to one year Also note any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for the removal, destruction of or blocking of access to the information referred to in this section. The Authority, on receipt of such application, may pass such orders as deemed appropriate. The Authority may also direct any of its licensees to secure such information including traffic data A fine which may extend to ten million rupees and/or imprisonment of up to five years

In regards to the extraterritorial reach of cybercrime legislation in Pakistan, Section 42 PECA states that the Federal Government may upon receipt of a request for co-operation, extend such cooperation to any foreign government, 24 x 7 network, foreign agency or international organization or agency. This is only for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under the PECA.

The Federal Government may also forward to a foreign government, 24 x 7 network, foreign agency or international agency or organization, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under the PECA. The Federal Government may also require the foreign government, 24 x 7 network, foreign agency or international agency to keep the information provided confidential or use it strictly for the purposes it is provided for.

Further, the Federal Government may send and answer requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

Where the Federal Government decides to provide the requested cooperation, the relevant requirements and safeguards provided under the PECA must be followed.

The Federal Government may however refuse to accede to any request made by a foreign government, 24 x 7 network, foreign agency, international organization or agency if:

(a) it is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interests of Pakistan;

(b) the offence is regarded by the Federal Government as being of a political nature;

(c) there are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons;

(d) the request relates to an offence, the prosecution of which in the requesting State may be incompatible with the laws of Pakistan;

(e) the assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offence been the subject of an investigation or prosecution under its own jurisdiction; or

(f) the request concerns an offence which may prejudice an ongoing investigation or trial or the rights of its citizens guaranteed under the Constitution.

The PECA also requires the designated agency to maintain a register of requests received from foreign governments, 24 x 7 networks, foreign agencies or international organizations or agencies.

Law stated as at 22 February 2017