[AS PASSED BY THE SENATE]

A

BILL

to make provisions for prevention of electronic crimes

WHEREAS it is expedient to prevent unauthorized acts with respect to information systems and provide for related offences as well as mechanisms for their investigation, prosecution, trial and international cooperation with respect thereof and for matters connected therewith or ancillary thereto:

It is hereby enacted as follows: -

CHAPTER I
PRELIMINARY

1. **Short title, extent, application and commencement**.- (1) This Act may be called the Prevention of Electronic Crimes Act, 2016.

(2) It extends to the whole of Pakistan.

(3) It shall apply to every citizen of Pakistan wherever he may be and also to every other person for the time being in Pakistan.

(4) It shall also apply to any act committed outside Pakistan by any person if the act constitutes an offence under this Act and affects a person, property, information system or data located in Pakistan.

(5) It shall come into force at once.

2. **Definitions**.- (1) In this Act, unless there is anything repugnant in the subject or context,

(a) "act" includes-

(i) a series of acts or omissions contrary to the provisions of this Act; or

(ii) causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device and whether having temporary or permanent impact;

(b) "access to data" means gaining control or ability to use, copy, modify or delete any data held in or generated by any device or information system;

(c) "access to information system" means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;

(d) "Authority" means the Pakistan Telecommunication Authority established under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);

(e) "authorization" means authorization by law or the person empowered to make such authorization under the law:

Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;

(f) "authorized officer" means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;

(g) "Code" means the Code of Criminal Procedure, 1898 (Act V of 1898);

(h) "content data" means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;

(i) "Court" means the Court of competent jurisdiction designated under this Act;

(j) "critical infrastructure" means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in:

(i) major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; or

(ii) significant impact on national security, national defense, or the functioning of the state".

Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of sub-paragraphs (i) and (ii) above, as critical infrastructure as may be prescribed under this Act.

(k) "critical infrastructure information system or data" means an information system, program or data that supports or performs a function with respect to a critical infrastructure;

(l) "damage to an information system" means any unauthorized change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system;

(m) "data" includes content data and traffic data;

(n) "data damage" means alteration, deletion, deterioration, erasure, relocation, suppression of data or making data temporarily or permanently unavailable;

(o) "device" includes-

(i) physical device or article;

(ii) any electronic or virtual tool that is not in physical form;

(iii) a password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or

(iv) automated, self-executing, adaptive or autonomous devices, programs or information systems;

(p) "dishonest intention" means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence;

(q) "electronic" includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology;

(r) "identity information" means an information which may authenticate or identify an individual or an information system and enable access to any data or information system;

(s) "information" includes text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) and codes including object code and source code;

(t) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;

(u) "integrity" means, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;

(v) "interference with information system or data" means and includes an unauthorized act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data;

(w) "investigation agency" means the law enforcement agency established by or designated under this Act;

(x) "minor" means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years;

(y) "offence" means an offence punishable under this Act except when committed by a person under ten years of age or by a person above ten years of age and under fourteen years of age, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion;

(z) "rules" means rules made under this Act;

(za) "seize" with respect to an information system or data includes taking possession of such system or data or making and retaining a copy of the data;

(zb) "service provider" includes a person who-

(i) acts as a service provider in relation to sending, receiving, storing, processing or distribution of any electronic communication or the provision of other services in relation to electronic communication through an information system;

(ii) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

(iii) processes or stores data on behalf of such electronic communication service or users of such service;

(zc) "subscriber information" means any information held in any form by a service provider relating to a subscriber other than traffic data;

(zd) "traffic data" includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;

(ze) "unauthorized access" means access to an information system or data which is not available for access by general public, without authorization or in violation of the terms and conditions of the authorization;

(zf) "unauthorized interception" shall mean in relation to an information system or data, any interception without authorization; and

(zg) "Unsolicited information" means the information which is sent for commercial and marketing purposes against explicit rejection of the recipient and does not include marketing authorized under the law.

(2) Unless the context provides otherwise, any other expression used in this Act or rules made thereunder but not defined in this Act, shall have the same meanings assigned to the expressions in the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898) and the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), as the case may be.

CHAPTER II
OFFENCES AND PUNISHMENTS

3. Unauthorized access to information system or data.- Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

4. Unauthorized copying or transmission of data.- Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both.

5. **Interference with information system or data**.- Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

6. **Unauthorized access to critical infrastructure information system or data**.-Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

7. **Unauthorized copying or transmission of critical infrastructure data.**- Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both.

8. **Interference with critical infrastructure information system or data**.- Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data , shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both.

9. **Glorification of an offence:-**(1) Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both.

Explanation.-"glorification" includes depiction of any form of praise or celebration in a desirable manner.

10. **Cyber terrorism**.–Whoever commits or threatens 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 proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

10A. Hate speech.- Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance inter-faith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

10B. Recruitment, funding and planning of terrorism.- Whoever prepares or disseminates information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plans for terrorism shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

11. Electronic forgery.- (1) Whoever interferes with or uses any information system, device or data, with the intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to two hundred and fifty thousand rupees or with both.

(2) Whoever commits offence under sub-section (1) in relation to a critical infrastructure information system or data shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to five million rupees or with both.

12. Electronic fraud.- Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.

13. Making, obtaining, or supplying device for use in offence.- Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to six months or with fine which may extend to fifty thousand rupees or with both.

14. Unauthorized use of identity information.-(1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both.

(2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.

15. Unauthorized issuance of SIM cards etc.- Whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices such as tablets, without obtaining and verification of the subscriber's antecedents 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.

16. Tampering, etc. of communication equipment.-Whoever unlawfully or without authorization changes, alters, tampers with or re-programs unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving information shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

Explanation.-A "unique device identifier" is an electronic equipment identifier which is unique to a communication device.

17. Unauthorized interception.- Whoever with dishonest intention commits 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

(a) electromagnetic emissions from an information system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

18. Offences against dignity of a natural person.- (1) Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

19. Offences against modesty of a natural person and minor.-(1) Whoever intentionally and publicly exhibits or displays or transmits any information which-

(a) superimposes a photograph of the face of a natural person over any sexually explicit image or video; or

(b) includes a photograph or a video of a natural person in sexually explicit conduct; or

(c) intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person; or

(d) cultivates, entices or induces a natural person to engage in a sexually explicit act,

through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both.

(2) Whoever commits an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term which may extend to seven years and with fine which may extend to five million rupees:

Provided that in case of a person who has been previously convicted of an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term of ten years and with fine.

(3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

19A. Child pornography.- (1) Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts-

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; or

(c) realistic images representing a minor engaged in sexually explicit conduct; or

(d) discloses the identity of the minor, shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both.

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

20. Malicious code.-Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent 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 shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or with both.

Explanation.-For the purpose of this section, the expression "malicious code" includes, a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorization.

21. Cyber stalking.- (1) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, 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.

(2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that if victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to five years or with fine which may extend to ten million rupees or with both.

(3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

22. Spamming.-(1) A person commits the offence of spamming, who with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain.

(2) A person including an institution or an organization engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing.

(3) Whoever commits the offence of spamming as described in sub-section (1) by transmitting harmful, fraudulent, misleading or illegal information, shall be punished with imprisonment for a term which may extend to three months or with fine of rupees fifty thousand which may extend upto rupees five million or with both.".

(4) Whoever commits the offence of spamming as described in sub-section (1) by transmitting unsolicited information, or engages in direct marketing in violation of sub-section (2), for the first time, shall be punished with fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with fine not less than fifty thousand rupees that may extend up to one million rupees.

23. Spoofing.-(1) Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing.

(2) Whoever commits spoofing 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.

24. Legal recognition of offences committed in relation to information system.- (1) Notwithstanding anything contained in any other law for the time being in force, an offence under this Act or any other law shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to or through the use of an information system.

(2) References to "property" in any law creating an offence in relation to or concerning property, shall include information system and data.

25. Pakistan Penal Code, 1860 (Act XLV of 1860) to apply.- The provisions of the Pakistan Penal Code, 1860 (Act XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act.

CHAPTER III
ESTABLISHMENT OF INVESTIGATION AGENCY AND PROCEDURAL POWERS FOR INVESTIGATION

26. Establishment of investigation agency.-(1) The Federal Government may establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act.

(2) Unless otherwise provided for under this Act, the investigation agency and the authorized officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act.

(3) The investigation agency shall establish its own capacity for forensic analysis of the data or information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency.

(4) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency.

27. Power to investigate.- Only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act: Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams comprising of an authorized officer of the investigation agency and any other law enforcement agency for investigation of an offence under this Act and any other law for the time being in force.

28. Expedited preservation and acquisition of data.- (1) If an authorised officer is satisfied that-

(a) specific data stored in any information system or by means of an information system is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible,

the authorized officer may, by written notice given to the person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice:

Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of acquisition of such data and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise.

(2) The period provided in sub-section (1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorized officer in this behalf.

29. Retention of traffic data.- (1) 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 production of a warrant issued by the court, provide that data to the investigation agency or the authorized officer whenever so required.

(2) The service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transactions Ordinance, 2002 (LI of 2002).

(3) Any owner of the information system who is not a licensee of the Authority and violates sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both:

Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996).

30. Warrant for search or seizure.- (1) Upon an application by an authorized officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that-

(a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or

(b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorize an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offence identified in the application.

(2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted officer of the investigation agency, may enter the specified place and search the premises and any information system, data, device or other articles relevant to the offence and access, seize or similarly secure any information system, data, device or other articles relevant to the offence:

Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.

31. Warrant for disclosure of content data.-(1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that the person in control of the data or information system, to provide such data or access to such data to the authorized officer.

(2) The period of a warrant issued under sub-section (1) may be extended beyond seven days if, on an application, a Court authorizes an extension for a further period of time as may be specified by the Court.

32. Powers of an authorized officer.-(1) Subject to provisions of this Act, an authorized officer shall have the powers to –

(a) have access to and inspect the operation of any specified information system;

(b) use or cause to be used any specified information system to search any specified data contained in or available to such system;

(c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system;

(d) have access to or demand any information in readable and comprehensible format or plain version;

(e) require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person;

(f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence under this Act; and

(g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence.

Explanation.-Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data.

(2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all times shall-

(a) act with proportionality;

(b) take all precautions to maintain integrity and secrecy of the information system and data in respect of which a warrant for search or seizure has been issued;

(c) not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued;

(d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and

(e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued.

(3) When seizing or securing any data or information system, the authorized officer shall make all efforts to use technical measures to maintain its integrity and chain of custody. The authorized officer shall seize an information system, data, device or articles, in part or in whole, as a last resort only in the event where it is not possible under the circumstances to use such technical measures or where use of such technical measures by themselves shall not be sufficient to maintain the integrity and chain of custody of the data or information system being seized.

(4) Where an authorized officer seizes or secures any data or information system, the authorized officer shall ensure that data or information system while in the possession or in the access of the authorized officer is not released to any other person including competitors or public at large and details including log of any action performed on the information system or data is maintained in a manner prescribed under this Act.

33. Dealing with seized data or information system.- (1) If any data or information system has been seized or secured following a search or seizure under this Act, the authorized officer who undertook the search or seizure shall, at the time of the seizure,–

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to-

(i) the occupier of the premises; or

(ii) the owner of the data or information system; or

(iii) the person from whose possession the data or information system has been seized, in a prescribed manner in the presence of two witnesses.

(2) The authorized officer, upon an application of the owner of the data or information system or an authorized agent of the owner and on payment of prescribed costs, shall provide forensic image of the data or information system to the owner or his authorized agent within a time prescribed under this Act.

(3) If the authorized officer has reasons to believe that providing forensic image of the data or information system to the owner under sub-section (2) may prejudice–

(a) the investigation in connection with which the search was carried out; or

(b) another ongoing investigation; or

(c) any criminal proceedings that are pending or that may be brought in relation to any of those investigations, the authorized officer shall, within seven days of receipt of the application under sub-section (2), approach the Court for seeking an order not to provide copy of the seized data or information system.

(4) The Court, upon receipt of an application from an authorized officer under sub-section (3), may after recording reasons in writing pass such order as deemed appropriate in the circumstances of the case.

(5) The costs associated with the exercise of rights under this section shall be borne by the person exercising these rights.

34. Unlawful on-line content.-(1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to an 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 this Act.

(2) The Authority shall, with the approval of the Federal Government, prescribe rules providing for, among other matters, safeguards, transparent process and effective oversight mechanism for exercise of powers under sub-section (1).

(3) Until such rules are prescribed under sub-section (2), the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act.

(4) Any person aggrieved from any order passed by the Authority under sub-section (1), may file an application with the Authority for review of the order within thirty days from the date of passing of the order.

(5) An appeal against the decision of the Authority in review shall lie before the High Court within thirty days of the order of the Authority in review.

35. **Limitation of liability of service providers**.- (1) No service provider shall be subject to any civil or criminal liability, unless it is established that the service provider had specific actual knowledge and willful intent to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider in connection with a contravention of this Act or rules made thereunder or any other law for the time being in force:

Provided that the burden to prove that a service provider had specific actual knowledge, and willful intent to proactively and positively participate in any act that gave rise to any civil or criminal liability shall be upon the person alleging such facts and no interim or final orders, or directions shall be issued with respect to a service provider by any investigation agency or Court unless such facts have so been proved and determined:

Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account ID), Uniform Resource Locator (URL), Top Level Domain (TLD), Internet Protocol Addresses (IP Addresses), or other unique identifier and clearly state the statutory provision and basis of the claim.

(2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith.

(3) No service provider shall be subject to any civil or criminal liability as a result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law:

Provided that the service provider, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served upon it by an authorized officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the authorized officer, the Court authorizes an extension for a further specified period upon being satisfied that reasonable cause for such extension exists.

(4) No service provider shall be liable under this Act, rules made thereunder or any other law for the disclosure of any data or other information that the service provider discloses only to the extent of the provisions of this Act.

(5) No service provider shall be under any obligation to proactively monitor, make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by such intermediary or service provider.

36. Real-time collection and recording of information.-(1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to information held by or passing through a service provider, to a designated agency as notified under the Investigation for Fair Trial Act, 2013 (I of 2013) or any other law for the time being in force having capability to collect real time information, to collect or record such information in real-time in coordination with the investigation agency for provision in the prescribed manner:

Provided that such 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.

(2) Notwithstanding anything contained in any law to the contrary the information so collected under sub-section (1) shall be admissible in evidence.

(3) 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.

(4) The Court may also require the designated agency to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.

(5) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also-

(a) explain why it is believed that the data sought will be available with 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 this Act 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) 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.

37. **Forensic laboratory**.- The Federal Government shall establish or designate a forensic laboratory, independent of the investigation agency, to provide expert opinion before the Court or for the benefit of the investigation agency in relation to electronic evidence collected for purposes of investigation and prosecution of offences under this Act.

38. **Confidentiality of information.-** Notwithstanding immunity granted under any other law for the time being in force, any person including a service provider while providing services under the terms of lawful contract or otherwise in accordance with the law, or an 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 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 confidentiality of such material or data shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that the burden of proof of any defense taken by an accused service provider or an authorized officer that he was acting in good faith, shall be on such a service provider or the authorized officer, as the case may be.

CHAPTER IV
INTERNATIONAL COOPERATION

39. International cooperation.- (1) The Federal Government may upon receipt of a request, through the designated agency under this Act, extend such cooperation to any foreign government, 24 x 7 network, any foreign agency or any international organization or agency 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 this Act.

(2) The Federal Government may forward to a foreign government, 24 x 7 network, any foreign agency or any 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 this Act.

(3) The Federal Government shall require the foreign government, 24 x 7 network, any foreign agency or any international organization or agency to keep the information provided confidential and use it strictly for the purposes it is provided.

(4) The Federal Government may, through the designated agency, send and answer requests for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution.

(5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any 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 interest 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 investigation or prosecution under its own jurisdiction; or

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

(6) Where the Federal Government decides to provide the requested cooperation, the relevant requirements and safeguards provided under this Act and rules framed thereunder shall be followed.

(7) The designated agency shall maintain a register of requests received from any foreign government, 24 x 7 network, any foreign agency or any international organization or agency under this Act and action taken thereon.

CHAPTER – V
PROSECUTION AND TRIAL OF OFFENCES

40. Offences to be compoundable and non-cognizable.-(1) All offences under this Act, except the offences under sections 10, 19 and 19A and abetment thereof, shall be non-cognizable, bailable and compoundable:

Provided that offences under section 15 shall be cognizable by the investigation agency on a written complaint by the Authority.

(2) Offences under sections 10, 19 and 19A and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency.

41. Cognizance and trial of offences.— (1) The Federal Government, in consultation with the Chief Justice of respective High Court, shall designate presiding officers of the Courts to try offences under this Act at such places as deemed necessary.

(2) The Federal Government shall, in consultation with the Chief Justice of respective High Court, arrange for special training of the presiding officers of the Court to be conducted by an entity notified by the Federal Government for training on computer sciences, cyber forensics, electronic transactions and data protection.

(3) Prosecution and trial of an offence under this Act committed by a minor shall be conducted under the Juvenile Justice System Ordinance, 2000 (XXII of 2000).

(4) To the extent not inconsistent with this Act, the procedure laid down under the Code and the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), shall be followed.

42. Order for payment of compensation.- (1) The Court may, in addition to award of any punishment including fine under this Act, make an order for payment of compensation to the victim for any damage or loss caused and the compensation so awarded shall be recoverable as arrears of land revenue:

Provided that the compensation awarded by the Court shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation so awarded.

43. Appointment of amicus curiae and seeking expert opinion.-The Court may appoint *amicus curiae* or seek independent expert opinion on any matter connected with a case pending before it.

44. Appeal.- An appeal against the final judgment or order of a Court shall , within thirty days from the date of provision of its certified copy free of cost, lie-

(a) to the High Court concerned against such judgment or order if passed by a court of sessions; or

(b) to the court of sessions concerned against such judgment or order if passed by a magistrate.

CHAPTER VI
PREVENTIVE MEASURES

45. Prevention of electronic crimes.-(1) The Federal Government or the Authority, as the case may be, may issue directives to be followed by the owners of the designated information systems or service providers in the interest of preventing any offence under this Act.

(2) Any owner of the information system who is not a licensee of the Authority and violates the directives issued under sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both.

Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996.

46. Computer emergency response teams.-(1) 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.

(2) A computer emergency response team constituted under sub-section (1) may comprise of technical experts of known expertise officers of any intelligence or agency or any sub-set thereof.

(3) 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.

CHAPTER VII
MISCELLANEOUS

47. Relation of the Act with other laws.- (1) The provisions of this Act shall have effect not in derogation of the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898), the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), the Protection of Pakistan Act, 2014 (X of 2014) and the Investigation for Fair Trial Act, 2013 (I of 2013).

(2) Subject to sub-section (1), the provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law on the subject for the time being in force.

48. Power to make rules.-(1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act.

(2) Without prejudice to the generality of the foregoing powers, such rules may specify-

(a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors;

(b) powers, functions and responsibilities of the investigation agency, its officers and prosecutors;

(c) standard operating procedures of the investigation agency;

(d) mode and manner in which record of investigation under this Act may be maintained;

(e) manner to deal with the seized data, information system, device or other articles;

(f) working of joint investigation teams;

(g) requirements for seeking permission of the Authority to change, alter or re-programme unique device identifier of any communication equipment by any person for research or any other legitimate purpose;

(h) procedure for seeking appropriate orders of the Authority for removal, destruction or blocking access to information under this Act;

(i) constitution of computer emergency response team and the standard operating procedure to be adopted by such team;

(j) appointment of designated agency having capability to collect real time information;

(k) manner of coordination between the investigation agency and other law enforcement and intelligence agencies including designated agency;

(l) for management and oversight of the forensic laboratory;

(m) qualifications and trainings of the officers, experts and staff of the forensic laboratory;

(n) powers, functions and responsibilities of the forensic laboratory, its officers, experts and staff;

(o) standard operating procedures of the forensic laboratory to interact with the investigation agency;

(p) manner of soliciting and extending international cooperation; and

(q) matters connected or ancillary thereto.

49. Removal of difficulties.- If any difficulty arises in giving effect to the provisions of this Act, the Federal Government may, within two years of the commencement of this Act and by order published in the official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty.

49A. The agency designated or established under section 26 of the Act shall submit a half yearly report to both houses of the Parliament for consideration by the relevant Committee in camera, in respect of its activities, without disclosing identity information, in a manner as prescribed under this Act.

50. Amendment of Electronic Transactions Ordinance, 2002 (LI of 2002) and pending proceedings.- (1) Sections 36 and 37 of the Electronic Transactions Ordinance, 2002 (LI of 2002) are omitted.

(2) Any action taken by or with the approval of the Authority or proceedings pending under the provisions of the Electronic Transactions Ordinance, 2002 (LI of 2002) repealed by sub-section (1), shall continue and be deemed to have been taken or initiated under this Act.

51. Savings of powers.-Nothing in this Act shall affect, limit or prejudice the duly authorized and lawful powers and functions of the institutions controlled by the Governments exercised and performed in good faith.

STATEMENT OF OBJECTS AND REASONS

Currently Pakistan has no law to comprehensively deal with the growing threat of cybercrime. The centuries old criminal justice legal framework is inadequate and ill equipped to address the sophisticated online threats of the 21st Century cyber age. While this new age has exacerbated both existing crimes when conducted with the use of the Internet, which are adequately addressed by the application of the Electronic Transactions Ordinance, 2002 in conjunction with existing criminal justice legislation, it has also given birth to completely new types of cybercrime and criminals which cannot be effectively dealt with through the use of exiting legislation. The latter cannot be addressed simply by amending existing legislation or through a patchwork of enabling provisions. The unique nature of these crimes finds no adequate or analogous provisions in existing legislation that deal with traditional offline crime. Effectively addressing these unique and unprecedented crimes with similarly unique and necessary procedural powers, requires a completely new and comprehensive legal framework that focuses on online conduct of individuals/organizations in the virtual world. The legislation therefore, establishes new offences including illegal access of data (hacking), as well as interference with data and information systems (DOS and DDOS attacks), specialized cyber related electronic forgery and electronic fraud, cyber terrorism (electronic or cyber attack on the critical information infrastructure), unauthorized interception conducted by civilians, use of malicious code viruses, identity theft etc.

The legislation provides new investigative powers hitherto unavailable such as search and seizure of digital forensic evidence using technological means, production orders for electronic evidence, electronic evidence preservation orders, partial disclosure of traffic data, real time collection of data under certain circumstances and other enabling powers which are necessary to effectively investigate cyber crime cases. The very technical nature of the new powers that are necessary to investigate and prosecute these crimes require their exercise to be proportionate with the civil liberty

protections afforded to citizens under the Constitution. This can only be achieved through strengthening existing protections and establishing new safeguards especially against abuse of these new and intrusive powers. The Bill also includes specific safeguards to balance against these intrusive and extensive procedural powers in order to protect the privacy of citizens and avoid abuse of the exercise of these powers.

The introduction of this legislation will effectively prevent cyber crimes and shall also contribute to the national security of the Nation whilst providing and enabling a secure environment or investment in IT, e-commerce and e-payments systems. This Bill shall also afford protection to citizens which has hitherto not been completely effective, exposing them to the unmitigated threats posed by cyber criminals both at home and abroad.

ANUSHA RAHMAN KHAN
Minister of State for Information Technology
Member-in-Charge