[Published in the Gazette of Pakistan, Extraordinary,
Part-I, dated the 5th November, 2008]

ORDINANCE NO. IX OF 2008

AN

ORDINANCE

to make provision for prevention of the electronic crimes

WHEREAS it is expedient to prevent any action directed against the confidentiality, integrity and availability of electronic system, networks and data as well as the misuse of such system, networks and data by providing for the punishment of such actions and to provide mechanism for investigation, prosecution and trial of offences and for matters connected therewith or ancillary thereto;

AND WHEREAS the National Assembly is not in session and President is satisfied that the circumstances exist which render it necessary to take immediate action;

NOW, THEREFORE, in exercise of the powers conferred by clause (1) of Article 89 of the Constitution of the Islamic Republic of Pakistan and in exercise of all powers enabling in that behalf, the President is pleased to make and promulgate the following Ordinance:—

1. **Short title, extent application and commencement.**—(1) This Ordinance may be called the Prevention of Electronic Crimes Ordinance, 2008.

(2) It extends to the whole of Pakistan.

(3) It shall apply to every person who commits an offence under this Ordinance irrespective of his nationality or citizenship whatsoever or in any place outside or inside Pakistan, having detrimental effect on the security of Pakistan or its nationals or national harmony or any property or any electronic system or data located in Pakistan or any electronic system or data capable of being connected, sent to, used by or with any electronic system in Pakistan.

(4) It shall come into force at once and shall be deemed to have taken effect on the 29th September, 2008

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

(a) "access" means gaining access to any electronic system or data held in an electronic system or by causing the electronic system to perform any function to achieve that objective;

(b) "Authority" means the Pakistan Telecommunication Authority established under section 3 of the Pakistan Telecommunication (Re-organization) Act 1996 (XVII of 1996);

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

(d) "Constitution" means Constitution of the Islamic Republic of Pakistan;

(e) "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including but not limited to computer program, text, images, sound, video and information within a database or electronic system;

(f) "decision of the Authority" means decision given, determination made or order passed by the Authority under any of the provisions of the Pakistan Telecommunication (Re-organization) Act 1996

(XVII of 1996) on any matter related to one or more licensed operators in pursuant to the powers conferred upon the Authority by any other law, rules, regulation or directive for the time being in force which includes any interim order passed by the Authority pending final decision;

(g) "Electronic Certification Accreditation Council" means the council established under section 18 of the Electronic Transaction Ordinance 2002 (LI of 2002);

(h) "electronic" includes but not limited to electrical, digital, analogue, magnetic, optical, biochemical, electrochemical, electromechanical, electromagnetic, radio electric or wireless technology;

(i) "electronic device" means any hardware which performs one or more specific functions and operates on any form or combination of electrical energy.

(j) "electronic mail message" means any data generated by an electronic system for a unique electronic mail address;

(k) "electronic mail address" means a destination, commonly expressed as a string of characters, consisting of a unique user or group name or mailbox, commonly referred to as the local part, and a reference to an internet or intranet domain, commonly referred to as the domain part, whether or not displayed, to which an electronic mail message can be sent or delivered or originated from the includes an electronic mail address which may be permanent, dynamic or disposable;

(l) "electronic system" means any electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program or manual or any external instruction, performs automatic processing of information or data and may also include a permanent, removable or any other electronic storage medium;

(m) "encrypted data" means data which has been transformed or scrambled from its plain version or text to any unreadable or incomprehensible format and is recoverable by an associated decryption or decoding technique, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting such data;

(n) "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system;

(o) "Interpol" means International Criminal Police Organisation;

(p) "offence" includes,—

(i) an offences punishable under this Ordinance;

(ii) an offence punishable under the laws mentioned in the Schedule; or

(iii) any other offence punishable under any other law for the time being in force if committed through or by using any computer, electronic system, electronic means or electronic device as a means or tool;

(q) "plain version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format or after it has been recovered by using any decryption or decoding technique;

(r) "rules" means rules made under this Ordinance;

(s) "Schedule" means the Schedule to this Ordinance;

(t) "sensitive electronic system" means an electronic system used directly in connection with or necessary for,—

(i) the security, defence or international relations of Pakistan;

(ii) the existence or identity of a confidential source of information relating to the enforcement of criminal law;

(iii) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation, public key infrastructure, payment systems infrastructure or e-commerce infrastructure;

(iv) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services;

(v) the purpose declared as such by the Federal Government in accordance with the prescribed procedure ; or

(vi) containing any data or database protected as such, by any other laws.

(u) "service provider" includes but not limited to,—

(i) a person acting as a service provider in relation to sending, receiving, storing or processing of electronic Communication or the provision of other services in relation to electronic communication through any electronic system;

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

(iii) any other person who processes or stores data on behalf of such electronic communication service or users or such services;

(v) "subscriber information" means any information contained in any form that is held by a service provider, relating to subscriber's services other than traffic data and by which can be established,—

(i) the type of communication service used, the technical provisions taken thereto and the period of services;

(ii) the subscriber's identity, postal geographic electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or

(iii) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

(w) "traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

(x) "Tribunal" means the Information and Communication Technologies Tribunal constituted under section 31; and

(y) "unauthorized access" means access of any kind by any person to any electronic system or data held in an electronic system or electronic device, without authority or in excess of authority, if he is not himself entitled to control access of the kind in question to the electronic system or electronic device, or data and he does not have consent to such access from any person, so entitled.

CHAPTER—II

OFFENCES AND PUNISHMENTS

3. **Criminal access.—** Whoever intentionally gains unauthorized access to the whole or any part of an electronic system or electronic device with or without infringing security measures, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees, or with both.

4. **Criminal data access.—**Whoever intentionally causes any electronic system or electronic device to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system or electronic device or on obtaining such unauthorized access shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

5. **Data damage.—**Whoever with intent to illegal gain or cause harm to the public or any person, damages any data is shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Explanation.—For the purpose of this section the expression "data damage" includes but not limited to modifying, altering, deleting, deterioration, erasing, suppressing, changing location of data or making data temporarily or permanently unavailable, halting electronic system, choking the networks or affecting the reliability or usefulness of data.

6. **System damage.—**Whoever with intent to cause damage to the public or any person interferes with or interrupts or obstructs the functioning, reliability or usefulness of an electronic system or electronic device by inputting, transmitting, damaging, deleting, altering, tempering, deteriorating or suppressing any data or services or halting electronic system or choking the networks shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Explanation.—For the purpose of this section the expression "services" include any kind of service provided through electronic system.

7. **Electronic fraud.**—Whoever for wrongful gain interferes with or uses any data, electronic system or electronic device or induces any person to enter into a relationship or with intent to deceive 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 of either description for a term which may extend to seven years, or with fine, or with both.

8. **Electronic forgery.**—Whoever for wrongful gain interferes with data, electronic system or electronic device, with 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 or not shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine or with both.

9. **Misuse of electronic system or electronic device.**—(1) Whoever produces, possesses, sells, procures, transports, imports, distributes or otherwise makes available an electronic system or electronic device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established under this Ordinance or a password, access code, or similar data by which the whole or any part of an electronic system or electronic devices is capable of being accessed or its functionality compromised or reverse engineered, with the intent that it be used for the purpose of committing any of the offences established under this Ordinance, is said to commit offence of misuse of electronic system or electronic devices:

Provided that the provisions of this section shall not apply to the authorized testing or protection of an electronic system for any lawful purpose.

(2) Whoever commits the offence described in sub-section (1) shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine or with both.

10. **Unauthorized access to code.**—Whoever discloses or obtains any password, access as to code, system design or any other means of gaining access to any electronic system or data with intent to obtain wrongful gain, do reverse engineering or cause wrongful loss to any person or for any other unlawful purpose shall be punished with imprisonment of either description for a term which may extend to three years, or with, or with both.

11. **Misuse of encryption.**—Whoever for the purpose of commission of an offence or concealment of incriminating evidence, knowingly and will fully encrypts any incriminating communication or data contained in electronic system relating to that crime or incriminating evidence, commits the offence of misuse of encryption shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both.

12. **Malicious code.**—(1) Whoever willfully writes, offers, makes available distributes or transmits malicious code through an electronic system or electronic device, with intent to cause harm to any electronic system or resulting in the corruption, destruction, alteration, suppression, theft or loss of data commits the offence of malicious code:

Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of an electronic system for any lawful purpose.

Explanation.—For the purpose of this section the expression "malicious code" includes but not limited to a computer program or a hidden function in a program that damages data or compromises the electronic system's performance or uses the electronic system resources without proper authorization, with or without attaching its copy to a file and is capable of spreading over electronic system with or without human intervention including virus, worm or Trojan horse.

(2) Whoever commits the offence specified I sub-section (1) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine or with both.

13. **Cyber stalking.**—(1) Whoever with intent to coerce, intimidate, or harass any person uses computer, computer network, internet, network site, electronic mail or any other similar means of communication to,—

(a) communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, picture or image;

(b) make any suggestion or proposal of an obscene nature;

(c) threaten any illegal or immoral act;

(d) take or distribute pictures or photographs of any person without his consent or knowledge; or

(e) display or distribute information in a manner that substantially increases the risk of harm or violence to any other person, commits the offence of cyber stalking.

(2) Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment of either description for a term which may extend to seven years or with fine not exceeding three hundred thousand rupees, or with both:

Provided if the victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to ten years or with fine not less than one hundred thousand rupees, or with both.

14. **Spamming.**—(1) Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited electronic messages in bulk to any person without the express permission of the recipient, or causes any electronic system to show any such message or involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming.

(2) Whoever commits the offence of spamming as described in sub-section (1) shall be punishable with fine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and for every subsequent commission of offence of spamming he shall be punished with imprisonment of three months or with fine or with both.

15. **Spoofing.**—Whoever establishes a website, or sends an electronic message with a counterfeit source intended to be believed by the recipient or visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information which later can be used for any unlawful purposes commits the offence of spoofing.

(2) Whoever commits the offence of spoofing specified in sub-section(1) shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

16. **Unauthorized interception.**—(1) Whoever without lawful authority intercepts by technical means, transmissions of data to, from or within an electronic system including electromagnetic emissions from an electronic system carrying such data commits the offence of unauthorized interception.

(2) Whoever commits the offence of unauthorized interception described in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine not exceeding five hundred thousand rupees, or with both.

17. **Cyber terrorism.**—(1) Any person, group or organization who, with terroristic intent utilizes, accesses or causes to be accessed a computer or computer network or electronic system or electronic device or by any available means, and thereby knowingly engages in or attempts to engage in a terroristic act commits the offence of cyber terrorism.

Explanation 1.—For the purposes of this section the expression "terroristic intent" means to act with the purpose to alarm, frighten, disrupt, harm, damage; or carry out an act of violence against any segment of the population, the Government or entity associated therewith.

Explanation 2.—For the purposes of this section the expression "terroristic act" includes. But is not limited to,—

(a) altering by addition, deletion, or change or attempting to alter information that may result in the imminent injury, sickness, or death to any segment of the population;

(b) transmission or attempted transmission of a harmful program with the purpose of substantially disrupting or disabling any computer network operated by the Government or any public entity;

(c) aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whether or not the commission of such act of violence is actually completed; or

(d) stealing or copying, or attempting to steal or copy, or secure classified information or data necessary to manufacture any form of chemical, biological or nuclear weapon, or any other weapon of mass destruction.

(2) Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable with death or imprisonment for life, and with fine and in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or with fine not less than ten million rupees, or with both.

18. **Enhanced punishment for offences involving sensitive electronic systems.**—(1) Whoever causes criminal access to any sensitive electronic system in the course of the commission of any of the offences established under this Ordinance shall, in addition to the punishment prescribed for that offence, be punished with imprisonment of either description for a term which may extend to ten years, or with fine not exceeding one million rupees, or with both.

(2) For the purposes of any prosecution under this section, it shall be presumed, until contrary is proved, that the accused had the requisite knowledge that it was a sensitive electronic system.

19. **Of abets, aids or attempts to commits offence.**—(1) Any person who knowingly and willfully abets the commission of or who aids to commit or does any act preparatory to or in furtherance of the commission of any offence under this Ordinance shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) Any person who attempts to commit an offence under this Ordinance shall be punished for a term which may extend to one-half of the longest term of imprisonment provided for that offence.

Explanation.—For aiding or abetting an offence to be committed under this section, it is immaterial whether the offence has been committed or not.

20. **Other offences.**—Whoever commits any offence, other that those expressly provided under this Ordinance, with the help of computer, electronic system, electronic device or any other electronic means shall be punished, in addition to the punishment provided for that offence, with imprisonment of either description for a term which may extend to two years, or with fine not exceeding two hundred thousand rupees, or with both.

21. **Offences by corporate body.**—A corporate body shall be held liable for an offence under this Ordinance if the offence is committed on its instructions or for its benefit. The corporate body shall be punished with fine not less than one hundred thousand rupees or the amount involved in the offence whichever is the higher:

Provided that such punishment shall not absolve the criminal liability of the natural person who has committed the offence.

Explanation.—For the purposes of this section corporate body, includes a body of persons incorporated under any law such as trust, waqf, an association, a statutory body or a company.

CHAPTER—III

PROSECUTION AND TRIAL OF OFFENCES

22. **Offences to be compoundable and non-cognizable.**—All offences under this Ordinance shall be compoundable, non-cognizable and bailable except the offences punishable with imprisonment for seven years or more.

23. **Prosecution and trial of offences.**—(1) The Tribunal shall take cognizance of and try any offence under this Ordinance.

(2) In all matters with respect to which no procedure has been provided in this Ordinance or the rules made thereunder, the provisions of the Code shall, *mutatis mutandis,* apply for the trial.

(3) All proceedings before the Tribunal shall be deemed to be judicial proceedings within the meanings of sections 193 and 228 of the Pakistan Penal Code 1860 (XLV of 1860) and the Tribunal shall be deemed to be a Court for the purposes of sections 480 and 482 of the Code.

24. **Order for payment of compensation.**—The Tribunal may, on awarding punishment of imprisonment or fine or both for commission of any offence, make an order for payment of any compensation to the victim for any damage caused to his electronic system or data by commission of the offence and the compensation so awarded shall be recoverable as arrears of and revenue:

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

CHAPTER IV

ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCIES

25. **Establishment of investigation agencies and prosecution.**—The Federal Government shall establish a specialized investigation and prosecution cell within Federal Investigation Agency to investigate and prosecute the offences under this Ordinance:

Provided that till such time any agency is so established, the investigation and prosecution of an offence shall be conducted in accordance with the provisions of the Code:

Provided further that any police officer investigating an offence under this Ordinance may seek assistance of any special investigation agency for any technical in put, collection and preservation of evidence.

26. **Powers of officer.**—(1) Subject to obtaining search warrant an investigation officer shall be entitled to,—

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

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

(c) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such electronic system into readable and comprehensible format or plain version;

(d) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any electronic system has been used;

(e) require any person having charge of, or otherwise concerned with the operation of such electronic system to provide him reasonable technical and other assistance as he may require for the purposes of clauses (a), (b) and (c);

(f) require any person who is in possession of decryption information of under investigation electronic system, device or data to grant him access to such decryption information necessary to decrypt data required 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 and from cipher text to its plain text.

(2) The police officer may, subject to the proviso, require a service provider to submit subscriber information relating to such services in respect of a person under investigation in the service provider's possession or control necessary for the investigation of the offence:

Provided the investigating officer shall get prior permission to investigate any service provider from the licensing authority where prior permission of the licensing authority is required under any law to investigate the licensed service provider.

(3) Any person who obstructs the lawful exercise of the powers under sub-sections (1) or (2) shall be liable to punishment with imprisonment of either description for a term which may extend to one year, or with fine not exceeding one hundred thousand rupees, or with both.

27. **Real-time collection of traffic data.**—(1) The Federal Government may require a licensed service provider, within its existing or required technical

capability, to collect or record through the application of technical means or to cooperate and assist any law enforcement or intelligence agency in the collection or recording of traffic data or data, in real-time, associated with specified communications transmitted by means of an electronic system.

(2) The Federal Government may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.

28. **Retention of traffic data.**—(1) A service provider shall, within its existing or required technical capability, retain its traffic data minimum for a period of ninety days and provide that data to the investigating agency or the investigating officer when required. The Federal Government may extend the period to retain such date as and when deems appropriate.

(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 Transaction Ordinance 2002 (LI of 2002).

(3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term of six months or with fine or with both.

29. **Trans-border access.**—For the purpose of investigation the Federal Government or the investigation agency may, without the permission of any foreign Government or international agency access publicly available electronic system or data, or access or receive, through an electronic system, data located in foreign country or territory, if it obtains the lawful and voluntary consent of the person who has the lawful authority to disclose it:

Provided that such access is not prohibited under the law of the foreign Government or the international agency:

Provided further that the investigating agency shall inform in writing to the Ministry of Foreign Affairs of Government of Pakistan and other relevant agencies as the case may be about the investigation conducted under this section.

CHAPTER-V

INTERNATIONAL COOPERATION

30. **International cooperation.**—(1) The Federal Government may cooperate with any foreign Government, Interpol or any other international agency with who it has or establishes reciprocal arrangements for the purposes of

investigations or proceedings concerning offences related to electronic system and data, or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of a electronic system or real-time collection of traffic data associated with specified communications or interception of data.

(2) The Federal Government may, without prior request, forward to such foreign Government, Interpol or other international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other Government or agency in initiating or carrying out investigations or proceedings concerning any offence.

(3) The Federal Government may require the foreign Government, Interpol or other international agency to keep the information provided confidential or use it subject to some conditions.

(4) The investigating agency shall, subject to approval of the Federal Government, be responsible for sending and answering 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 such foreign Government, Interpol or international agency if the request concerns an offence which is likely to prejudice its sovereignty, security, public order or other essential interests.

(6) The Federal Government may postpone action on a request if such action would prejudice investigations or proceedings conducted by its investigation agency.

CHAPTER—VI

INFORMATION AND COMMUNICATION TECHNOLOGIES TRIBUNAL

31. **Information and Communication Technologies Tribunal.—**(1) As soon as possible after the commencement of this Ordinance, the Federal Government shall, by notification in the official Gazette, constitute the Information and Communication Technologies Tribunal whose principal seat shall be at Islamabad.

(2) The Tribunal may hold its sittings at such place or places as the Federal Government may decide.

(3) The Tribunal shall consist of a chairman and as many members as the Federal Government may determine but not more than seven members.

(4) The Chairman may constitute Benches of the Tribunal and unless otherwise directed by him a Bench shall consist of not less than two members. A Bench shall exercise such powers and discharge such functions as may be prescribed. There shall be established at least one Bench in each province.

(5) The Federal Government shall appoint the Chairman and members of the Tribunal.

32. **Qualifications for appointment.—**(1) A person shall not be qualified for appointment as Chairman unless he is, or has been, or is qualified for appointment as a judge of the High Court.

(2) A person shall not be qualified for appointment as a Member unless he—

(a) has for two years served as a District and Sessions Judge;

(b) has for a period of not less than ten years been an advocate of a High Court; or

(c) has special knowledge of legislation and professional experience of not less than ten years in the field of telecommunication and information technologies.

33. **Salary and allowances, and other terms and conditions of services.—**The salary, allowance, privileges, and the other terms and conditions of service o the Chairman and member of the Tribunal shall be such as the Federal Government may, by notification on official Gazette, determine.

34. **Resignation and removal.—**(1) The Chairman or a member of the Tribunal may, by writing under his hand addressed to the Federal Government, resign his office:

Provided that the Chairman or a member shall, unless he is permitted by the Federal Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such resignation or until a person duly appointed as his successor enters upon his office whichever is earlier.

(2) The Chairman or a member of the Tribunal shall not be removed from his office before the expiry of term specified in section 33, by the Federal Government except as may be prescribed.

(3) The Federal Government may, by rules, regulate the procedure for the investigation of misconduct or physical or mental incapacity of the Chairman and a member of the Tribunal.

35. **Saving Tribunal's proceedings.—**No act or proceedings of the Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of the Tribunal.

36. **Employees of the Tribunal.—**(1) The Federal Government shall provide the Tribunal with such employees as the Government may deem appropriate in consultation with the Chairman of the Tribunal.

(2) The employees of the Tribunal shall perform their duties under general superintendence of the Chairman of the Tribunal.

(3) The salaries, allowances and other conditions of service of the employees of the ICT Tribunal shall be such as may be prescribed by the Federal Government.

37. **Right to legal representation.—**The parties in appeal may either appear in person or authorize one or more legal practitioners, and in case of a corporate body any of its officers, to present the case before the Tribunal.

38. **Amicus curiae.—**(1) The Tribunal may, if it so requires, be assisted in technical aspects in any case by an amicus curiae having knowledge and experience in information communication technologies, finance and economics.

(2) The Federal Government shall maintain a list of amicus curiae having relevant qualifications and experience.

(3) The Tribunal in consultation with the Federal Government shall determine the remuneration of the amicus curiae and the Tribunal may decide the party or parties to pay such remuneration, keeping in view the circumstances of each case.

39. **Procedure and powers of Tribunal.—**(1) Subject to the provision of this Ordinance and the rules made thereunder, the Tribunal,—

(i) may, where it deems necessary, apply the procedures as provided in the Code or, as the case may be, in the Code of Civil Procedure, 1908 (Act V of 1908);

(ii) in the exercise of its civil jurisdiction, shall have powers vested in the civil court under the Code of Civil Procedure, 1908; and

(iii) in the exercise of its criminal jurisdiction, shall have the same powers as are vested in the Court of Session under the Code.

40. **Appeal to Tribunals.—**(1) Any person aggrieved by any of the following orders may, within fifteen days 'from the date of such order, prefer an appeal to the Tribunal, namely:—

(a) any decision of the Authority; or

(b) any decision of the Electronic Certification Accreditation Council:

Provided that no appeal shall lie to the ICT Tribunal from an order passed by the Authority or the Electronic Certification Accreditation Council with the consent of the parties.

(2) Any appeal against a decision of the Authority shall be accompanied by a court fee,—

(a) ten thousand rupees where the valuation of the subject matter in issue is not more than five million rupees;

(b) fifty thousand rupees where the valuation of the subject matter in issue is more than five million rupees but not more than then million rupees; and

(c) one hundred thousand rupees where the valuation of the subject matter in is more than ten million rupees.

(3) The appeal filed before the Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and the Tribunal shall dispose of the appeal finally within ninety days from the date of receipt of the appeal.

41. **Powers of Tribunal.—**The Tribunal while hearing an appeal under section 40 shall have all the powers as are vested in the court of first appeal under the Code in exercise of its civil jurisdiction in respect of appeal against any decision or order of the Authority or the Electronic Certification Accreditation Council.

42. **Limitation.—**The provisions of the Limitation Act, 1908 (IX of 1908), shall, *mutatis mutandis*, apply to the proceedings of ICT Tribunal.

43. **Appeal to High Court.—**(1) Any person aggrieved by—

(i) any decision or order of the Tribunal made under section 40 may prefer second appeal to the respective High Court within thirty days from the date of the decision or order of the Tribunal:

Provided that appeal under this clause shall lie only if the High Court grants leave to appeal;

(ii) an order of conviction passed by the Tribunal in respect of any offence under this Ordinance may prefer an appeal to the respective High Court within thirty days of the decision or order of the Tribunal.

(2) An appeal against an order of the Tribunal under section 40 or an order of sentence exceeding ten years shall be heard by the Division Bench of the High Court.

44. **Civil court not to have jurisdiction.**—No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Tribunal constituted under this Ordinance is empowered by or under this Ordinance to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Ordinance.

45. **Transitory proceedings.**—(1) Until the establishment of the Tribunal all cases, proceedings and appeals, subject matter of which is within the jurisdiction of Tribunal, shall continue to be heard and decided by the competent forum existing under any law for the time being in force.

(2) On the constitution of the Tribunal all cases, proceedings and appeals shall stand transferred to and heard and disposed of by the Tribunal.

(3) On transfer of cases, proceedings and appeals under sub-section (2), the Tribunal shall proceed from the stage the proceedings had reached immediately prior to the transfer and shall not be bound to recall any witness or again record any evidence that may have been recalled.

CHAPTER—VII

MISCELLANEOUS

46. **Ordinance to override other laws.**—The provisions of this Ordinance shall have effect notwithstanding anything to the contrary contained in any other law for the time being in force.

47. **Power to amend Schedule.**—The Federal Government many, by notification in the official Gazette, amend the Schedule so as add any entry thereto or modify or omit any entry therein.

48. **Power to amend Schedule.**—(1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of the Tribunal.

49. **Removal of difficulties.**—If any difficulty arises in giving effect to the provisions of this Ordinance, the Federal Government may, by order published in the official Gazette, make such provisions not inconsistent with the provisions of this Ordinance as may appear to be necessary for removing the difficulty.

THE FIRST SCHEDULE

[See section 2(p)(ii)]

1. The Electronic Transactions Ordinance, 2002 (LI of 2002)

2. The Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996).

3. The Telegraph Act, 1885 (XIII of 1885).

4. The Wireless Telegraphy Act, 1933 (XVII of 1933).

STATEMENT OF OBJECTS AND REASONS

A wide array of new and complex Information and Communication Technologies (ICT) related crimes are not covered under any of the existing legislation; therefore, to counter the spread of electronic crimes, there is an urgent need for having a legislation for prevention of electronic crimes in Pakistan to check electronic crimes ranging from damage to data and electronic system, electronic fraud and forgery, unauthorized access to code and misuse of encryption, cyber stalking, spamming, spoofing, unauthorized interception and cyber terrorism. This law also provides a comprehensive mechanism for investigation, prosecution and trial's procedures for prevention of electronic crimes.

2. By establishing a proper mechanism of investigation, prosecution and trial for electronic crimes in the field of Information and Communication Technologies, *inter alia* :

(a) a sense of security, safety and protection will prevail in each and every segment of society that uses or deals with IT and Telecommunication;

(b) increasing rate of electronic crimes in the country will be curbed ;

(c) soft image of Pakistan will be developed in the world;

(d) the confidence of Bankers and their customers in electronic transactions will be enhanced which consequently will boost e-Banking and e-Commerce in Pakistan;

(e) the IT entrepreneurs will have more secure cyber space which will be friendly and congenial to their business;

(f) Pakistan will be able to take another step further towards paper free economy; and

(g) it will promote the whole ICT sector and build confidence in the society to accept the use of more and more Information and Communication Technologies in their daily lives.

3. The Bill seeks to achieve the aforesaid objects.

MINISTER – IN- CHARGE