ACT No.____ OF 2014

AN

ACT

To make provision for prevention of electronic crimes

WHEREAS it is expedient to prevent unauthorised 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;

It is hereby enacted as follows:-

1. **Short title, extent application and commencement**.-(1) This Act may be called the Prevention of Electronic Crimes Act, 2014.

(2) It extends to the whole of Pakistan.

(3) It shall also apply notwithstanding the matters being the subject hereof occurring outside Pakistan, in so far as they are directly or indirectly connected to, or have an effect on or bearing in relation to persons, information systems or events within the territorial jurisdiction of Pakistan.

(4) it shall come into force at once.

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

(a) "access" means gaining access to the whole or any part of any information system whether or not through enabling entry, control or the right to use the whole or any part of any information system;

(b) “access to program or data” means access to any program or data held in any information systems if by causing an information system to perform any function whereby a person —

(i) alters, modifies or erases the program or data or any aspect or attribute related to the program or data; or

(ii) copies, transfers or moves it to-

a. any information system, device or storage medium other than that in which it is held; or

b. to a different location in the same information system, device or storage medium in which it is held; or

(iii) uses it; or

(iv) has it output from the information system in which it is held, whether by having it displayed or in any other manner;

Provided that for the purposes of clause b (iii) above a person uses a program if the function he causes the information system to perform—

(i) causes the program to be executed; or

(ii) is itself a function of the program.

Provided further that for the purposes of clause b (iv) above—

(i) a program is output if the instructions of which it consists are output; and

(ii) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by an information system) is immaterial.

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

(d) "content data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable to cause an information system to perform a function:

Provided that such content data is other than traffic data and does not include traffic data:

Provided further that the content data shall only include and be limited to content data related to identified subscribers or users who are the subject of an investigation or prosecution and with respect of whom any warrant under this Act has been issued:

Provided also that the content data is restricted to content data a service provider actually holds itself and does not include any content data that is not held by the service provider itself;

(e) “the Court” means the Court of Sessions competent to try offences under this Act;

(f) “critical infrastructure” means the assets, systems and networks, whether physical or virtual, so vital to the Government that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.

(g) "critical infrastructure information system, program or data" means any information system, program or data that supports or performs a function with respect to a critical infrastructure.

(h) "designated payment system" means designated payment system as defined under clause (q) of section 2 of the Payment Systems and Electronic Fund Transfers Act, 2007.

(i) "device" includes-

(i) physical device or article;

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

(iii) any program or data held in electronic form;

(iv) 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

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

(j) "electronic" means electronic as defined under clause (l) of section 2 of the Electronic Transactions Ordinance, 2002 (LI of 2002);

(k) "Federal Government" means the Federal Government in the Ministry of Interior, unless for any specific purpose specified otherwise by notification in the official Gazette notification or amendment in the Rules of business, 1973;

(l) "identity information" means any information including biological or physiological information of a type that is generally used alone or in combination with other information to verify, authenticate or identify or purport to verify, authenticate or identify an individual or an information system, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, mother's maiden name, challenge phrase, security question, written signature, advanced electronic signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, National Identity Card Number, customer number, driver's licence number, any password, any biometric method or any other form of verification, authentication or identification that may have become available because of modern devices or techniques and which may enable access to any information system or to the performance of any function or interference with any computer data or an information system.

(m) "information" means information system as defined under clause (o) of section (2) (o) of the Electronic Transactions Ordinance, 2002 (LI of 2002)

(n) "information system" means information system as defined under clause (p) of section (X) of the Electronic Transactions Ordinance, 2002 (LI of 2002);

(o) “investigating officer” means an officer of the special investigation agency established under section 16 of this Act;

(p) “negligence” shall mean unreasonable conduct that creates an obvious risk of harm or damage through genuine inadvertence;

(q) "offence" means an offence punishable under this Act;

(r) references to an act by a “person” shall include acts done or to be done:

(i) by or through automated mechanisms and self-executing, adaptive or autonomous devices, programs or information systems;

(ii) against Government controlled information systems or public information systems in exercise of a public function, or

(iii) against any information system

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

(t) "Schedule" means the Schedule to this Act;

(u) “seize” with respect to program or data includes-

(i) seize or similarly secure an information system or part of it or a device; or

(ii) make and retain a copy of any program or data, including by using on-site equipment; or

(iii) render inaccessible, or remove, data in the accessed information system; or

(iv) obtain output of data from an information system;

(v) "service provider" includes-

(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;

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

(iv) any person who, as a core business or a substantial part of his business provides premises from where and facilities through which the public in

general may as customers access information systems and the internet such as cyber cafes; or

(v) any person who, as a core business or a substantial part of his business, provides a network for distribution of electronic communication;

(w) "subscriber information" means any information contained in any form that is held by a service provider, relating to a service of a subscriber 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 service;

(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:

Provided that subscribers for the purpose of this Act shall only include and be limited to those subscribers who are the subject of an investigation or prosecution and with respect of whom any warrant under this Act has been issued:

Provided further that the subscriber information is restricted to the information a service provider actually holds itself and does not include any information that is not held by the service provider itself;

(x) "traffic data" means any available data relating to a communication by means of an information system, generated by an information system that formed a part in the chain of communications, indicating the communication's origin, destination, route, time, data, size, duration or type of underlying service, actually held by the service provider itself and does not include any data that is not held by the service provider itself;

(y) "unauthorized" for the purposes of section 3 shall mean access of any kind by any person to any information system if-

(i) he is not himself entitled to control access of the particular kind or type in question with respect to an information system; and
(ii) he does not have consent of the person entitled to grant such consent, for the particular kind or type of access in question with respect to an information system;

Provided that access in exercise of powers under sections 19, 21, 23, 30, 32 and 48 shall not be deemed to be unauthorized;

(z) "unauthorized" for the purposes of section 4 shall mean access of any kind by any person to any program or data if —

(i) he is not himself entitled to control access of the particular kind or type in question with respect to that program or data; and

(ii) he does not have consent of the person entitled to grant such consent, for the particular kind or type of access in question with respect to that program or data:

Provided that access to program or data in exercise of powers under sections 19, 21, 23, 30, 32 and 48 shall not be deemed to be unauthorized.

(aa) "unauthorised act" means in relation to an information system, a program or data, an act where the person doing the act or causing it to be done—

(i) is not the person with the responsibility for the information system;

(ii) is not the person who is entitled to determine whether the act may be done; and

(iii) does not have consent to the act from the person with the responsibility for the information system; and

(ab) "unauthorised interception" shall mean in relation to an information system, program or data, any interception where the person intercepting or causing interception to take place—

(i) is not the person with the responsibility for the information system;

(ii) is not the person who is entitled to determine whether such interception may take place; and

(iii) does not have consent for such interception from the person with the responsibility for the information system.

(2) For the purposes of this Act and of any offence a person acts-

(a) "knowingly" with respect to a circumstance not only when he is aware that it exists or will exist, but also when he avoids taking steps that might confirm his belief that it exists or will exist;

(b) "intentionally" with respect to-

(i) a circumstance when he hopes or knows that it exists or will exist; and

(ii) a result when he acts either in order to bring it about or being aware that it will occur in the ordinary course of events;

(c) "recklessly" with respect to-

(i) a circumstance when he is aware of a risk that it exists or will exist; and

(ii) a result when he is aware of a risk that it will occur; and

(iii) it is, in the circumstances known to him, unreasonable to take the risk:

Provided that the threshold required to satisfy the burden of proof for proving the *mens rea* of recklessness shall be lower than that required when proving intention but higher than that required for negligence:

Provided further that the standard applied to test the state of mind of the person shall be the subjective standard which shall take into account the individual characteristics of the person including his age, background, experience and understanding.

These and related words (such as "knowledge", "intention", "recklessness") shall be construed accordingly unless the context otherwise requires.

Explanation.- Recklessness refers to a person's conscious or advertent taking of an unjustified risk when he carries out a deliberate act, knowing or closing his mind to the obvious fact that there is some risk resulting from that act but nevertheless continues in the performance of that act. The test to satisfy the mens rea shall be subjective in nature taking into account the individual characteristics of an accused including his age, background, experience and understanding. The subjective test shall require taking into account the actual ability of the accused to perceive a risk, taking into account his characteristics. If his ability, based on his characteristics, is less than that of a reasonable person then it shall be his ability that shall be relevant (subjective standard), instead of the standard applied to a hypothetical reasonable person who might have better knowledge and understanding (objective standard) than the person in question.

CHAPTER I
OFFENCES AND PUNISHMENTS

3. **Illegal access to information system**.- (1) Whoever intentionally, whether temporary or not,—

(a) causes an information system to perform any function with intent to secure access to the whole or any part of any information system or to enable any such access to be secured;

(b) the access he intends to secure or to enable to be secured is unauthorized under this section; and

(c) at the time when he causes the information system to perform the function he knows that the access he intends to secure or to enable to be secured is unauthorized under this section,

shall be punished with imprisonment of either description for a term which may extend to six months or with fine which may extend to one hundred thousand rupees or with both.

Explanation.-The absence of authority in this section will also include instances where there may exist general authority to access an information system but a specific type, nature or method of access may not be authorised.

Illustrations.-

(a) A, an employee of B, is authorised by B to generally access and use B's information system at A's place of employment. A is not authorised by B generally, or with respect to any specific type, nature or kind of information to make any copies of, transfer or transmit any information. The employee makes copies of such information, transfers or transmits such information. The act of accessing the information system for the purpose of such copying, transferring, transmitting would amount to access without authority.

(b) A, an employee of B, is authorised by B to generally access and use B's information systems at A's place of employment. A is not authorised by B to connect any data storage device to any of B's information systems. A connects a data storage device to B's information system. Such access by A of B's information system is without authority.

(2) Whoever recklessly, whether temporarily or not,—

(a) causes an information system to perform any function with intent to secure access to the whole or any part of any information system or to enable any such access to be secured;

(b) the access he intends to secure, or to enable to be secured, is unauthorized under this section; and

(c) at the time when he causes the information system to perform the function he knows that the access he intends to secure, or to enable to be secured, is unauthorized under this section,

shall be punished with imprisonment of either description for a term which may extend to three months or with fine which may extend to fifty thousand rupees, or with both.

Illustrations:

(a) A, an employee of B, is authorised by B to generally access and use B's information system at A's place of employment. A is not authorised by B generally, or with respect to any specific type, nature or kind of information to, make any copies, transfer or transmit any information. The employee whilst browsing the network accesses any part of an information system which he knows he is not authorised to access but does not have a specific intent to access such part of the information system but without such specific intent takes positive steps to access such a part(s) of the information system. Such access would be illegal access with recklessness but not intentional.

(b) A, an employee of B, is authorised by B to generally access and use B's information systems at A's place of employment. A is not authorised by B to connect any data storage device to any of B's information systems. A connects a data storage device to B's information system. Such access by A of B's information system is without authority.

(3) The intention referred to in sub-section (1) or the recklessness referred to in sub-section (2) above, need not relate to—

(a) any particular information system;

(b) any particular program or data; or

(c) a program or data of any particular kind.

4. **Illegal access to program or data**.- (1) Whoever intentionally, whether temporarily or not,—

(a) causes access to any program or data to be secured or to be enabled;

(b) the access to the program or data he intends to secure, or to enable to be secured, is unauthorized under this section; and

(c) at the time when he accesses the program or data he knows that the access he intends to secure, or to enable to be secured, is unauthorized under this section.

shall be punished with imprisonment of either description for a term which may extend to nine months or with fine which may extend to two hundred thousand rupees, or with both.

(2) Whoever recklessly, whether temporarily or not,—

(a) causes access to any program or data to be secured or to be enabled;

(b) the access to the program or data he intends to secure, or to enable to be secured, is unauthorized under this section; and

(c) at the time when he accesses the program or data he knows that the access he intends to secure, or to enable to be secured, is unauthorized under this section.

shall be punished with imprisonment of either description for a term which may extend to six months or with fine which may extend to one hundred thousand rupees, or with both.

Illustrations:

(a) A, an employee of B, is authorised by B to generally access and use B's information system at A's place of employment. A is not authorised by B generally, or with respect to any specific type, nature or kind of information to, make any copies of, transfer or transmit any information. The employee, whilst browsing the network, accesses program or data which he knows he is not authorised but does not have a specific intent to access such program or data but

without such specific intent takes positive steps to access such program or data. Such access would be illegal access with recklessness but not intentional.

(b) A, an employee of B, is authorised by B to generally access and use B's information systems at A's place of employment. A is not authorised by B to connect any data storage device to any of B's information systems. A connects a data storage device to B's information system. Such access by A of B's information system is without authority.

(3) The intention referred to in sub-section (1), or the recklessness referred to in sub-section (2), need not relate to—

(a) any particular information system;

(b) any particular program or data; or

(c) a program or data of any particular kind.

5. **Illegal interference with program or data**.- (1) Whoever intentionally, whether temporarily or not, —

(a) does any unauthorised act in relation to an information system;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) acts with intent—

(i) to destroy, damage, delete, erase, deteriorate, generate, modify or alter any program or data;

(ii) to render any program or data inaccessible, meaningless, useless or ineffective;

(iii) to obstruct, interrupt or interfere with any program or data or any aspect or attribute related to the program or data;

(iv) to obstruct, interrupt or interfere with any person in the use of any program or data or any aspect or attribute related to the program or data;

(v) to deny, prevent, suppress or hinder access to any program or data to any person entitled to it;

(vi) to deny, prevent, suppress or hinder access to any program or data or any aspect or attribute related to the program or data or make it inaccessible;

(vii) to impair the operation of any program or any aspect or attribute related to the program;

(viii) to impair the reliability of any data or any aspect or attribute related to the data;

(ix) to impair the security of any program or data or any aspect or attribute related to the program or data; or

(x) to enable any of the things mentioned in sub-clauses (i) to (ix) to be done,

shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to five hundred thousand rupees, or with both.

(2) Whoever recklessly, whether temporarily or not, —

(a) does any unauthorised act in relation to an information system;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) acts recklessly thereby–

(i) causing destruction, damage, deletion, erasure, deterioration generation, modification or alteration of any program or data or any aspect or attribute related to the program or data;

(ii) rendering any program or data meaningless, useless or ineffective;

(iii) obstructing, interrupting or interfering with the use of any program or data or any aspect or attribute related to the program or data;

(iv) obstructing, interrupting or interfering with any person in the use of any program or data or any aspect or attribute related to the program or data;

(v) causing denial, prevention, suppression or hindrance of access to program or data or any aspect or attribute related to the program or data to any person entitled to it;

(vi) causing denial, prevention, suppression or hindrance of access to any program or data or any aspect or attribute related to the program or data;

(vii) causing impairment to the operation of any program;

(viii) causing impairment to the reliability of any data or any aspect or attribute related to the program or data;

(ix) causing impairment to the security of any program or data or any aspect or attribute related to the program or data;

(x) causing enablement of any of the things mentioned in sub-clauses (i) to (ix) to be done,

shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to two hundred and fifty thousand rupees or with both.

(3) Whoever commits any offence under sub-section (1) by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

(4) Whoever commits any offence under sub-section (2) by circumventing or infringing security measures with respect to any information system, program or 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 two hundred and fifty thousand rupees or with both.

(5) Whoever commits any offence under sub-section (1) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to seven years or with fine which may extend to seven million rupees or with both.

(6) Whoever commits any offence under sub-section (2) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to four years or with fine which may extend to three million rupees or with both.

(7) The intention referred to in sub-section (1) or the recklessness referred to in subsection (2) need not relate to—

(a) any particular information system;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(8) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily;

(d) a reference to an act by a person includes acts done or to be done-

(i) by or through an automated mechanism and self-executing, adaptive or autonomous device, program or information system;

(ii) against Government controlled information systems or public information systems in exercise of a public function, or

(iii) against any information system:

Provided that an act under sections 19, 21, 23, 30, 32 and 48 shall not be deemed to be unauthorized.

6. **Illegal interference with information system**.- (1) Whoever intentionally, whether temporarily or not, —

(a) does any unauthorised act in relation to an information system;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) acts with intent to severely—

(i) interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct the functioning of an information system;

(ii) interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct communication between or with an information system;

(iii) interfere with or hinder access to any information system;

(iv) impair the operation of any information system;

(v) impair the reliability of any information system;

(v) impair the security of any information system; or

(vi) to enable any of the things mentioned in sub-clauses (i) to (v) to be done

shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

(2) Whoever recklessly, whether temporarily or not, —

(a) does any unauthorised act in relation to an information system;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) acts recklessly thereby causing severe–

(i) interference, hindrance, damage, prevention, suppression, deterioration or obstruction to the functioning of an information system;

(ii) interference, hindrance, damage, prevention, suppression, deterioration, impairment or obstruction of communication between or with an information system;

(iii) interference or hindrance to the access of any information system;

(iv) impairment to the operation of any information system;

(v) impairment to the reliability of any information system;

(vi) impairment to the security of any information system: or

(vii) to enable any of the things mentioned in sub-clauses (i) to (vi) to be done

shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to two hundred and fifty thousand rupees or with both.

(3) Whoever commits any offence under sub-section (1) by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

(4) Whoever commits any offence under sub-section (2) by circumventing or infringing security measures with respect to any information system, program or 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 two hundred and fifty thousand rupees or with both.

(5) Whoever commits any offence under sub-section (1) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to seven years or with fine which may extend to seven million rupees or with both.

(6) Whoever commits any offence under sub-section (2) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to four years or with fine which may extend to three million rupees or with both

(7) Whoever commits any offence under sub-section (1)

(a) with respect to any Government controlled or public information system, program or data that performs a public function ; and

(b) that causes serious damage, injury or disruption to a widely and publicly utilised network of information systems,

shall be punished with imprisonment of either description for a term which may extend to ten years or with fine which may extend to ten million rupees or with both.

(8) Whoever commits any offence under sub-section (2) -

(a) with respect to any Government controlled or public information system, program or data that performs a public function ;and

(b) that causes serious damage, injury or disruption to a widely and publicly utilised network of information systems,

shall be punished with imprisonment of either description for a term which may extend to seven years or with fine which may extend to seven million rupees or with both.

(9) The intention referred to in sub-section (1), or the recklessness referred to in sub-section (2), need not relate to—

(a) any particular information system;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(10) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily;

(d) a reference to an act by a person in this section includes acts done or to be done:

(i) by or through an automated mechanisms and self-executing, adaptive or autonomous devices, programs or information systems;

(ii) against Government controlled information systems or public information systems in exercise of a public function, or

(iii) against any information system:

Provided that an act under sections 19, 21, 23, 30, 32 and 48 shall not be deemed to be unauthorized.

7. **Cyber terrorism**. – (1) Whoever commits or threatens to commit any of the offences under sub-sections (1), (3) and (5) of section 5 and sub sections (1), (3), (5) and (7) of section 6 where-

(a) the use or threat is designed to coerce, intimidate, overawe or 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 in society; or

(b) the use or threat is made for the purpose or motive of advancing a cause whether political, religious, sectarian or ethnic, with the intention of:

(i) interfering with, disrupting or damaging a public utility service or a communications system used by the public at large;

(ii) severe interference with, seriously disrupting or seriously damaging a designated payment system which interconnects with multiple financial institutions;

(iii) severe interference with, seriously disrupting or seriously damaging a mass transportation or mass traffic system;

(iv) severe interference with, seriously disrupting or seriously damaging a critical infrastructure that is used to serve a public function for the public at large;

(v) severe interference with, seriously disrupting or seriously damaging critical infrastructure in use by the armed forces, civil armed forces, security forces or law enforcement agencies;

(vi) causes injury through the acts mentioned in clauses (i), (iii), (iv) and (v); or

(vii) enabling any of the things mentioned in sub-clauses (i) to (vi) to be done,

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.

(2) Whoever commits any offence under sub-section (1) of this section by circumventing or infringing security measures with respect to any information system, program or data 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.

(3) The intention referred to in sub-section (1) need not relate to—

(a) any particular information system;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(4) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily;

(d) a reference to an act by a person includes acts done or to be done-

(i) by or through an automated mechanism and self-executing, adaptive or autonomous device, program or information system;

(ii) against Government controlled information systems or public information systems in exercise of a public function: or

(iii) against any information system.

8. **Electronic forgery**.- (1) Whoever,-

(a) without authority;

(b) in excess of authority; or

(c) through an unauthorised act,

inputs, generates, alters, modifies, deletes or suppresses data, resulting in inauthentic data or an inauthentic program with the intent that it be considered or acted upon, by any person or an information system, as if it were authentic or genuine, regardless whether or not the data is directly readable and intelligible, shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to two hundred and fifty thousand rupees or with both.

(2) Whoever commits an offence under subsection (1), dishonestly or with similar intent, -

(a) for wrongful gain;

(b) for wrongful loss; or

(c) for any economic benefit for oneself or for another person,

shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to two hundred and fifty thousand rupees or with both.

(3) Whoever commits an offence under subsection (1), fraudulently, dishonestly or with similar intent, -

(a) to influence a public servant in the exercise of a public duty or function; or

(b) to influence a Government controlled information system or public information system in exercise of a public function,

shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

9. **Electronic fraud**.- Whoever with fraudulent or dishonest intent-

(a) without authority;

(b) in excess of authority; or

(c) through an unauthorised act,

causes loss, in whole or in part, of any data or program, property, valuable security or consideration to another person or any information system by-

(a) any illegal access to information system or illegal access to program or data;

(b) any input, alteration, modification, deletion, suppression or generation of any program or data;

(c) any interference, hindrance, impairment or obstruction with the functioning of an information system; or

(d) copying, transferring or moving any data or program to any information system, device or storage medium other than that in which it is held or to a different location in the any other information system, device or storage medium in which it is held; or uses any data or program; or has any data or program output from the information system in which it is held, whether by having it displayed or in any other manner;

with fraudulent or dishonest intent to cause-

(i) wrongful gain;

(ii) wrongful loss; or

(iii) any economic benefit for oneself or for another person,

shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to ten million rupees but shall not be less than the wrongful loss caused to any person or with both.

10. **Making, supplying or obtaining devices for use in offence**.-(1) Whoever produces, makes, generates, adapts for use any device intending it primarily be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under sections 3, 4, 5, 6, 7, 8, 9, 11, 12 or 14, shall be punished with imprisonment of either description for a term which may extend to 6 months or with fine which may extend to fifty thousand rupees or with both.

(2) Whoever transfers, imports, exports, distributes, shares, supplies, offers to supply or otherwise makes available any device believing that it is to be primarily used to commit or to assist in the commission of an offence under sections 3, 4, 5, 6, 7, 8, 9, 11, 12 or 14, shall be punished with imprisonment of either description for a term which may extend to one year or with fine which may extend to one hundred thousand rupees or with both.

(3) Whoever acquires, obtains or procures any device with a view to its being supplied for primarily to be used to commit or to assist in the commission of an offence under sections 3, 4, 5, 6, 7, 8, 9, 11, 12 or 14, shall be punished with imprisonment of either description for a term which may extend to one year or with fine which may extend to one hundred thousand rupees or with both:

Provided that it shall not be an offence under this section-

(a) where the production, making, adaptation, sale, procurement for use, import, distribution or otherwise making available of such device referred to in this section is not for the purpose of committing an offence under this Act: or

(b) any act under this section is for the authorised training, testing or protection of an information system.

11. **Identity crime**.- (1) Whoever knowingly obtains or possesses another person's identity information, without lawful justification, in circumstances giving rise to an inference that is established beyond reasonable doubt that the information is intended to be used to commit an offence that includes dishonesty, fraud, deceit or falsehood as an element of the offence shall, unless the contrary is proved, be punished with imprisonment of either description for a term which may extend to three months or with fine which may extend to fifty thousand rupees, or with both.

(2) Whoever transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an offence that includes fraud, deceit or falsehood as an element of the offence shall be punished with imprisonment of either description for a term which may extend to six months or with fine which may extend to one hundred thousand rupees or with both.

12. **Unauthorized interception**.-(1) Whoever intentionally commits unauthorized interception by technical means of-

(a) any transmission that is not intended to be and is not open to the public to, from or within an information system; or

(b) 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:

Provided that it shall not be an offence if interception is undertaken in compliance of and in accordance with the terms of a warrant issued under this Act or if lawfully conducted by any intelligence agency or intelligence service mentioned under section 48 of this Act:

Provided further that this section shall not have any application upon the activities and functions of intelligence agencies or services and is without prejudice to national security requirements, and laws identified under section 48 of this Act.

(2) Whoever commits an offence under sub-section (1) fraudulently, dishonestly or with similar intent shall be punished with imprisonment of either description for a term which may extend to four years or with fine which may extend to one million rupees or with both.

(3) Whoever commits an offence under sub-section (2) fraudulently, dishonestly or with similar intent -

(a) for wrongful gain; or

(b) for wrongful loss; or

(c) for any economic benefit for oneself or for another person,

shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to five million rupees or with both.

13. **Special protection of women.**- Whoever, with malicious intent, knowingly publicly exhibits, displays, transmits any electronic communication that harms the reputation of a woman, threatens any sexual acts against a woman; superimposes a photograph of the face of a woman over any sexually explicit images; distorts the face of a woman; or includes a photograph or a video of a woman in sexually explicit conduct, without the express or implied consent of the woman in question, intending that such electronic communication cause that woman injury or threatens injury to her reputation, her existing state of privacy or puts her in fear for her safety shall be punished with imprisonment for a term which may extend to one year or with fine which may extend to one million rupees or with both:

Provided that it shall not be an offence under this section if the electronic communication is an expression of opinion in good faith not done with malicious intent, is an expression of criticism, satire or political comment or is analogous to any of the Exceptions under section 499 of the Pakistan Penal Code Act, 1908:

Provided further that the term "woman" in this section refers to any female regardless of her age who must either be a complainant herself or in the event that she is a minor, her legal guardian must be the complainant.

14. **Of abetments, aids or attempts to commit 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 Act 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 Act 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.

15. **Legal recognition of offences committed in relation to information systems**.- (1) Notwithstanding anything contained in any other law, 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 electronic information, information systems, programs and the information and data contained in or conveyed through such information systems.

(3) References in any law creating an offence to an act shall include actions taken or caused by use of an information system.

(4) References to an act by a person in this Act or any law establishing an offence shall include acts done or to be done-

(a) by or through automated mechanisms and self-executing, adaptive or autonomous devices, programs or information systems;

(b) against Government controlled information systems or public information systems in exercise of a public function; or

(c) against any information system.

CHAPTER II
ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCY AND PROCEDURAL POWERS FOR INVESTGATION

16. **Establishment of investigation agencies and prosecution**.-(1) The Federal Government shall designate the Federal Investigation Agency or designate any other law enforcement agencies as the special investigation agency for the purposes of investigation and prosecution of offences under this Act.

(2) Unless otherwise provided for under this Act the special investigation agency, the special investigating officer, prosecution and the court 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:

Provided that any police officer investigating an offence under this Act may seek assistance of the special investigation agency for any technical or forensic analysis of evidence.

(3) All investigating officers appointed under this Act or exercising any power, privilege, right or provision under this Act shall, at a minimum, hold a specialized qualification in digital forensics, information technology or computer science, in such terms as may be prescribed.

17. **No warrant, arrest, search, seizure or other power not provided for in the Act**.- (1) No person whether a police officer, investigation officer or otherwise, other than an investigating officer of the special investigation agency shall investigate an offence with respect to, in connection with or under this Act.

(2) No person other than a prosecutor assigned by the special investigating agency shall prosecute any offence with respect to, in connection with or under this Act.

(3) No court lower than the Court of Sessions, in accordance with the provisions of this Act in particular section 37, shall conduct the trial, hearing of all proceedings in respect of, related to or in connection with an offence under this Act.

(4) No person, other than an investigating officer of the special investigation agency, shall exercise any power, including but not limited to arrest, access, search, seizure, preservation, production or real time collection or recording, under this Act, rules made thereunder or any other law, with respect to and in connection with any offence under this Act.

(5) No investigating officer shall exercise any power of arrest, access, search, seizure, preservation, production, or real time collection other than a power provided for under this Act.

(6) Notwithstanding any other law including sections 94 and 95 of CHAPTER VII Part B of the Code or any other provision of any law, and without prejudice to and subject at all times to sections 19, 20, 21, 29 and 30 of this Act, no investigating officer shall conduct any inquiry or investigation or call for any information in connection with any offence under this Act without obtaining an order for the disclosure of such information from the Court and the Court shall only issue such order if the particulars of the investigation meet the qualification provided for under the relevant section of this Act to which the request for disclosure pertains.

(7) Any investigating officer, when mentioning any section of this Act in any application or any document, including but not limited to any application for any warrant or disclosure under this Act or any report under sections 154, 155 or 173 or any other provision of the Code or any other law with respect to any investigation, inquiry, arrest, access, search, seizure, preservation, production, or real time collection under this Act, shall not merely mention the section but shall also specify the subsection and sub clause to identify exactly which offence is being referred to.

18. **Expedited Preservation of data**.- (1) If an investigating officer is satisfied that-

(a) traffic data or content 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 traffic data or content data may be modified, lost, destroyed or rendered inaccessible,

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

(2) The period of preservation and maintenance of integrity may be extended beyond seven days if, on an application by the investigating officer, the Court authorizes an extension for a further specified period of time, upon being satisfied that reasonable cause for such extension exists.

(3) The person in control of the information system shall only be responsible to preserve the data specified-

(a) for the period of the preservation and maintenance of integrity notice or for any extension thereof permitted by the Court;

(b) to the extent that such preservation and maintenance of integrity will not be administratively or financially burdensome; and

(c) where it is technically and practically reasonable to preserve and maintain the integrity of such data.

19. **Warrant for search and seizure**.-(1) Upon an application on oath by an investigating 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, program, data, device or storage medium of a specified kind that-

(a) is reasonably 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 after recording reasons, issue a warrant which shall authorise an investigation officer, with such assistance as may be necessary, to enter in the presence of a Magistrate, only the specified place and to search only the specified information system, program, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure only the specified data or specified program, device or storage medium relevant to the offence identified in the application, but without causing any of the results identified in sub-clause (c) of sub-section (1) of section 5 and in any event without prejudicing the integrity and security of any data or program available in or through the specified information system, program or generally present or available at the specified place:

Provided that the Magistrate for the purposes of this Chapter shall not include any person who is employed or performs any function on behalf of the special investigating agency:

(2) The application under subsection (1) shall in addition to substantive grounds and reasons also:

(a) explain why it is believed the material sought will be found on the premises to be searched;

(b) why the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them;

(c) identify and explain with specificity the type of evidence suspected will be found on the premises;

(d) identify and explain with specificity the relevant program or data that is sought and reasonably suspected to be available from each individual information system, device or storage medium;

(e) identify and explain with specificity the relevant individual information systems, devices or storage mediums expected to be searched or seized and reasonably suspected to contain the relevant program or data or any evidence;

(f) what measures shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of information systems or devices;

Provided that this shall not prejudice the powers defined in subs-section 3 of section 21;

(g) describe and identify the persons to be authorised to accompany the officer executing the warrant and the reasons that necessitate their presence; and

(h) seek the Court to depute a Magistrate who will be accompanying the officer during execution of the warrant.

(3) No court shall issue any warrant to enter and search any specific premises, any specific information system or any specific program or any specific data or any specific device or any specific storage medium unless satisfied that consequent upon the particulars of the offence referred to in the application, there are reasonable grounds for believing that it is necessary to search any specific premises occupied, any specific information system or any specific program or any specific data or any specific device or any specific storage medium controlled by the person identified in the application in order to find the material sought.

(4) Any person who obstructs the lawful exercise of the powers under sub-section (1) or sub-section (2) or misuses the powers granted under this section shall be liable to punishment with imprisonment of either description for a term which may extend to one month, or with fine not exceeding fifty thousand rupees, or with both.

Provided that it shall not be an offence for a person to refuse cooperation if that person is a suspect or accused or is by exercise of such power being compelled to incriminate himself, provide or procure information or evidence or be a witness against himself.

20. **Warrant for disclosure of traffic data**.-(1) Upon an application on oath by an investigating officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that specified data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to a specifically identified offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system disclose sufficient traffic data about a specified communication to identify-

(a) the service providers; and

(b) the path through which the communication was transmitted.

(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.

(3) The application under sub-section (1) shall in addition to substantive grounds and reasons also:

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

(b) identify and explain with specificity the type of traffic data suspected will be found on such information system;

(c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such information system;

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

(e) what measures shall be taken to prepare and ensure that the traffic data will be sought and carried out

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data of any party not part of the investigation.

(4) Any person who obstructs the lawful exercise of the powers under sub-section (1) or sub-section (2) or misuses the powers granted under this section shall be liable to punishment with imprisonment of either description for a term which may extend to one month or with fine not exceeding fifty thousand rupees or with both:

Provided that it shall not be an offence for a person to refuse cooperation if that person is a suspect or accused or is by exercise of such power being compelled to incriminate himself, provide or procure information or evidence or be a witness against himself.

21. **Powers of an investigating officer**.-(1) Subject to obtaining a search warrant under section 19 an investigation officer shall be entitled to only the information system, program and data specified in the warrant to-

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

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

(c) obtain and copy that data, use equipment to make copies and obtain an intelligible output from an information system.

(d) 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 information system into readable and comprehensible format or plain version;

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

(f) require any person having charge of or otherwise concerned with the operation of such information system to provide him reasonable technical and other assistance as the investigating officer may require for the purposes of clauses (a), (b) and (c); 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 decryption information necessary to decrypt data required for the purpose of investigating any such offence:

Provided that this power shall not empower an investigating officer to compel a suspect or an accused to provide decryption information, or to incriminate himself or provide or procure information or evidence or be a witness against himself.

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

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

(a) at all times act with proportionality;

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

(c) not disrupt or interfere with the integrity or running and operation of any information system, program 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 subject of the search or seizure; 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 similarly securing any data, the investigating officer shall make all efforts to use technical measures to copy or replicate the data, whilst maintaining its

integrity and chain of custody and shall only seize any information system, device or storage medium physically, in whole or in part, as a last resort, for sufficient reasons that do not make it possible under the circumstances to use such technical measures or where use of such technical measures by themselves would not be sufficient to maintain the integrity and chain of custody of the data being seized:

Provided that where a physical seizure occurs, the investigating officer shall submit forthwith and in any event no later than twenty four hours a report detailing sufficient reasons for such seizure before the Court.

22. **Cordons for investigation**. --- (1) Upon obtaining a warrant under section 19, an area is a cordoned area for the purposes of an investigation under this Act, if it is designated as such under this section.

(2) A designation may be made only by an investigating officer specially designated in this respect by the specialized investigation agency, if he considers it expedient for the purposes of the investigation.

(3) If a designation is made orally, the officer making it shall confirm it in writing, as soon as is reasonably practicable.

(4) The officer making a designation shall arrange for the demarcation of the cordoned area, so far as is reasonably practicable.

(5) An area may be designated a cordoned area for a period not exceeding fourteen days, which may be extended in writing from time to time, with each extension specifying the additional period:

Provided that a designation shall have no effect after twenty eight days beginning with the day on which it was made.

(6) Any cordoning under this section shall adequately take into consideration and provide for the avoidance of any interruption, obstruction, hindrance or disruption to continued legitimate business operations and the premises or area so cordoned.

(7) Any person affected by such cordoning may seek the removal or modification or the cordoning before the Court and the Court shall consider, when passing any order in this respect no later than seven days, make such order that avoids any interruption, obstruction or hindrance or disruption to continued legitimate business operations without prejudice to the preservation and integrity of evidence in the case.

(8) Where a person knows or has reasonable cause to suspect that an investigation is being conducted or is proposed to be conducted, a person commits an offence if he interferes with material which is likely to be relevant to an investigation and shall be liable on conviction to imprisonment for a term not less than six months and not exceeding two years, and fine:

Provided that it is a defence for a person charged with an offence under sub-section (8) to prove that he did not know and had no reasonable cause to suspect that the disclosure or interference was likely to affect an investigation.

Explanation. For the purposes of this section a person interferes with any material if he falsifies it, conceals it, destroys it or disposes of it or if he causes or permits another to do any of these things.

23. **Dealing with seized data.-**(1) If data has been seized or similarly secured, following a search or a seizure under section 19, the investigating officer who undertook the search shall, at the time of the search or as soon as practicable after the search with respect to the data seized-

(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 person in control of the information system; or

(iii) a person having any legal right to the data.

(2) Subject to sub-section (3), at the time of the search and in any event not later than twenty-four hours following the seizure, the investigating officer shall-

(a) permit a person who had the custody or control of the information system or someone acting on their behalf to access and copy data on the information system; or

(b) give the person a copy of the data.

(3) The investigating officer or another authorized person may refuse to give access or provide copies if the investigating officer has reasonable grounds for believing that giving the access or providing the copies-

(a) would constitute a criminal offence; or

(b) would prejudice-

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

(ii) another ongoing investigation; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

(4) The Court may, on the application of:

(a) the occupier of the premises; or

(b) the person in control of the information system, or

(c) a person with any legal right to the data,

on being shown sufficient cause, order that a copy be provided to such a person.

(5) The costs associated with the exercise of rights under sub-sections (2) and (4) shall be borne by the person exercising these rights.

24. **Dealing with seized physical information systems**.-(1) If an information has been physically seized or similarly secured, following a search or a seizure under section 18, the investigating officer who undertook the search must, at the time of the search or in any event no later than twenty-four hours after the seizure, with respect to the physical information systems seized,-

(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 person in control of the information system; or

(iii) a person with any legal right to the data.

(2) Subject to sub-section (3), on request, an investigating officer or another authorized person must, at the time of the search or as soon as practicable after the search,-

(a) permit a person who had the custody or control of the information system, or someone acting on their behalf to access and copy data on the information system; or

(b) give the person a copy of the data.

(3) The investigating officer or another authorized person may refuse to give access or provide copies if the investigating officer has reasonable grounds for believing that giving the access, or providing the copies-

(a) would constitute a criminal offence; or

(b) would prejudice-

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

(ii) another ongoing investigation; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

(4) The Court may on the application of-

(a) the occupier of the premises; or

(b) the person in control of the information system, or

(c) a person with any legal right to the data,

on being shown sufficient cause, order that a copy be provided to such a person.

(5) The costs associated with the exercise of rights under sub-sections (2) and (4) shall be borne by the person exercising these rights.

25. **Warrants for arrest**.– (1) No person shall be arrested or detained with respect to or in connection with any offence under this Act unless a warrant for arrest has been issued by the Court under this section.

(2) Upon an application on oath by an investigating officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that a specified person identified in the application has committed or participated in the commission of an offence under this Act, the Court may, after recording reasons, issue a warrant which shall authorise an investigation officer, with such assistance as may be necessary, to arrest the person identified in the application.

(3) The application under sub-section (1) shall in addition to substantive grounds and reasons also-

(a) explain why it is reasonably believed that the person identified in the application committed or participated in the commission of an offence under this Act;

(b) identify and explain with specificity the type of evidence so far available which leads the investigating officer to reasonably suspect that the person identified in the application is reasonably suspected of either having committed or participated in the commission of an offence under this Act;

(c) identify and explain with specificity the source of the evidence or information so far available which leads the investigating officer to reasonably suspect that the person identified in the application committed or participated in the commission of an offence under this Act;

(d) what measures shall be taken to prepare and ensure that the arrest is carried out with the use of reasonable and proportionate force; and

(e) what measures shall be taken to safeguard the unnecessary publicity of the identity of the person identified in the application and safeguarding the privacy of the family of the person identified in the application;

(4) No court shall issue any warrant to arrest any person unless satisfied that consequent upon the particulars of the offence referred to in the application, there are reasonable grounds for believing that the person identified in the application has committed an offence under this Act.

(5) Any person who obstructs the lawful exercise of the powers under sub-section (1) or sub-section (2) shall be liable to punishment with imprisonment of either description for a

term which may extend to one month or with fine not exceeding fifty thousand rupees or with both.

(6) Simultaneous to the arrest of the person identified in the application the investigating officer shall inform such person that-

(a) he has the right to remain silent;

(b) anything he says can and shall be used against him in the court of law;

(c) he has the right to communicate and consult with an advocate as well as have his advocate present at all times during and when any questioning or when making a statement or confession; and

(d) if he cannot afford an advocate he may elect to have the specialized investigation agency immediately appoint an advocate for him and subsequently also have the Court appoint a different advocate for him, if so elects, when he appears before the Court next morning.

(7) No person other than the investigating officer or a member of any joint investigation team shall have the right to question the person arrested under this Act.

(8) No person arrested under this Act shall be denied the right of access and presence of his advocate before and during any questioning.

(9) Any person arrested under this Act shall have the right to-

(a) not make any statement;

(b) not answer any questions;

(c) to remain silent; and

(d) have his advocate present.

(10) Any person arrested under this Act shall have the right without being compelled, to waive any of the rights mentioned above and such waiver and evidence of there being no compulsion shall be documented through video and audio recording.

(11) Notwithstanding anything contained in the Qanoon-e-Shahadat, 1984 (President's Order No. 10 of 1984) or any other law for the time being in force, where in any Court proceedings held under this Act the evidence, which includes circumstantial and other evidence, produced raises the presumption that there is a reasonable probability that the accused has committed the offence, any confession made by the accused during investigation without being compelled, before a Magistrate or an investigation officer specially designated by the specialized investigation agency in this respect, may be admissible in evidence against him, if such confession is documented through video and audio recording and demonstrates that the accused was under no compulsion in this regard:

Provided that the investigating officer before recoding any such confession, shall have explained to the person making the confession of his rights under this Act and that he is not under any compulsion whether direct or indirect to make a confession and that if he does so it may be used as evidence against him:

Provided further that no investigating officer shall record such confession unless, upon questioning the person making it the investigating officer had reason to believe that it was made voluntarily; and that when he recorded the confession, he made a memorandum at the foot of such record to the following effect, namely:-

'I have explained to (…name…) that:

(a) he has a right to remain silent

(b) anything he says can and shall be used against him in the court of law;

(c) that he has the right to communicate and consult with an advocate as well as have his advocate present at all times during an when being questioned or making any statement or confession

(d) if he cannot afford an advocate he may elect to have the specialized investigation agency immediately appoint an advocate for him and subsequently also have the Court appoint a different advocate for him, if he so elects, when he appears before the Court next morning.

(e) he is not under any compulsion whether direct or indirect to make any statement or any confession

(f) if he does make a statement or confession can and shall be used as evidence against him which would open him to being convicted of an offence.

Before making the statement of confession I had seen to it that the person making it was left in isolation without the presence of any investigating officer or other person that may influence him being present. I have also checked his body to see if there exist any signs of torture and my findings are mentioned herein. I believe that this confession was voluntarily made without any direct or indirect compulsion. It was taken in my presence and was read over to the person making it and admitted by him to be correct and it contains a full and true account of the statement made by him. My explanation to the person making the confession and his entire statement of confession has been documented through video and audio recording without any break or interruption in the recording.

(Signed)
Investigating officer / Magistrate.'

Explanation. It shall not be necessary that the Magistrate or specially designated investigation officer receiving and recording a confession or statement should be a Magistrate having jurisdiction in the case or an investigation officer involved in the investigation of the case.

(12) Only evidence of statements or questioning conducted and documented through video and audio recording shall be admitted before any Court whether as evidence or otherwise.

26. **Limitation of liability of intermediaries and service providers**.- (1) No intermediary or service provider shall be subject to any civil or criminal liability, unless it is finally established that the intermediary or service provider had actual notice, specific actual knowledge, willful and malicious intent and motive 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 an intermediary or service provider in connection with a contravention of this Act, rules made thereunder or any other law:

Provided that the burden to prove that an intermediary or service provider had notice, specific actual knowledge, willful and malicious intent and motive 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, directions shall be issued with respect to any intermediary or service provider unless such facts have so been finally 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 intermediary or 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.

(3) No intermediary or 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 intermediary or service provider present and established in terms equivalent to the requirements of the Companies Ordinance 1984 within the territorial jurisdiction of Pakistan, 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 them by an investigating officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the investigating officer, the Court authorizes an extension for a further specified period of time, upon being satisfied that reasonable cause for such extension exists.

(4) No intermediary or 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 and under sub-section (3) n and sections 18, 19, 20 and 21.

(5) No intermediary or 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.

27. **Immunity against disclosure of information relating to security procedure**.—(1) Subject to sub-section (2), no person shall be compelled to disclose any password, key or other secret information exclusively within his private knowledge, which enables his use of the security

procedure or advanced electronic signature.

(2) Subject to the right against self-incrimination under sub-section (2) of section 161 of the Code and Article 13 (2) of the Constitution, sub-section (1) shall not confer any immunity where such information is used for the commission of any offence under this Act, rules made thereunder or any other law.

28. **Inadmissibility of seized evidence**.- (1) Any evidence seized or similarly secured through any violation or failure to comply with any of the provisions of this Act shall have the effect of tainting the evidence seized and such evidence shall not be admissible before any Court or authority for any purpose in the relevant proceedings or any other proceedings.

(2) No evidence shall be accessed, searched, seized or similarly secured unless it is relevant to the offence identified in the application and the warrant issued which shall superficially identify the particular evidence to be searched or seized is issued.

(3) An application to declare evidence inadmissible for the purposes of sub-section (1) or for any other reason may be moved at any time during the criminal proceedings whether during the stage of inquiry, investigation, trial, before judgment or in appeal.

29. **Information of offence**.- (1) On receiving any complaint or information with respect to any offence under this Act, the investigating officer shall immediately enter the information in a book to be kept by such officer in such form as the Provincial Government may prescribe in this behalf under section 155 of the Code.

(2) A copy of the information entered under sub-section (1) shall be submitted no later than twenty-four hours before the court having jurisdiction in the matter which shall thereafter take cognizance of the matter and proceed in accordance with the Code.

(3) No inquiry, investigation, arrest, search, seizure shall take place or other power exercised, nor shall any warrant for search, seizure, arrest or exercise of other power be issued unless the provisions of this section are satisfied.

(4) No investigating officer shall investigate any case under this Act without the order of the Court of competent jurisdiction under this Act having power to try such case.

(5) The provisions of this section shall apply notwithstanding any other law and shall survive any amendments of any other law unless specifically amended or repealed.

30. **Real-time collection and recording of data**.-(1) If a Court is satisfied on the basis of information on oath on an application by an investigating officer that there are reasonable grounds to believe that the content of any specifically identified electronic communications is reasonably required for the purposes of a specific criminal investigation, the Court may order with respect to traffic data held by or content data that may pass through a service provider within its jurisdiction, through application of technical means, to-

(a) have that service provider collect or record traffic data in real-time; and

(b) and where administratively and financially not burdensome and technically possible, collect or record content data in real-time, conducted only through, in coordination with and facilitated by the intelligence agency or intelligence service referred to in section 48

of this Act and specially notified in respect of and for the purposes of this section by the Federal Government through notification in the Official Gazette,

associated with only the specified communications and related to or connected with only the person under investigation transmitted by means of an information system and provide only the specified traffic data and where applicable content data, to the investigating officer:

Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event not for more than seven days.

(2) 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 of time:

Provided that any extensions will require a full rehearing of the matter and the standard for satisfaction of the Court shall be higher with every application for extension.

(3) The Court 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.

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

(a) explain why it is believed the traffic data and where applicable content data sought will be available with the person in control of the information system;

(b) identify and explain with specificity the type of traffic data and where applicable content data suspected will 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) what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of information and data of any party not part of the investigation;

(f) 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:

Provided that the standard to be satisfied before the Court under sub-section (1) shall be that of beyond reasonable doubt and in any event a higher standard than that applicable to orders under sections 19, 20 and 25 of this Act.

Provided further that the application for exercise of powers under this section shall exclusively be made before the High Court having territorial jurisdiction in the matter under investigation, prosecution or trial and any reference in this section to "Court" shall mean the High Court having territorial jurisdiction in the matter under investigation, prosecution or trial.

Provided further that the real time collection or recording of content data shall only be conducted through and in coordination with and facilitated by the intelligence agency or intelligence service referred to in section 48 of this Act and notified for the purpose and in respect of this section by the Federal Government by notification in the Official Gazette.

31. **Retention of traffic data**.-(1) A service provider shall, within its technical capability, retain its traffic data minimum for a period of ninety days.

(2) The service provider 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).

32. **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 information system or data notwithstanding the geographical location of such information 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.

CHAPTER III
INTERNATIONAL COOPERATION

33. **International cooperation**.-(1) The Federal Government may cooperate with any foreign Government, 27 x 7 network, any foreign agency or any international 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 of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of an information system or real-time collection of traffic data associated with specified communications or interception of data or any other means, power, function or provision under this Act.

(2) The Federal Government may, without prior request, forward to such foreign Government, 27 x 7 network, any foreign agency or any 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, 27 x 7 network, any foreign agency or any international agency to keep the information provided confidential or use it subject to some conditions.

(4) The investigating agency shall 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, 27 x 7 network, any foreign agency or any international agency if the request concerns an offence which is likely to prejudice its sovereignty, security, public order or other national 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 – IV
PROSECUTION AND TRIAL OF OFFENCES

34. **Offences to be compoundable and non-cognizable**.-All offences under this Act shall be compoundable, non-cognizable and bailable.

Provided that the offence under section 7 shall be non-bailable and non-compoundable.

35. **Prosecution and trial of offences**.—No Court inferior to the Court of Sessions Court shall try any offence under this Act.

(2) In all matters with respect to which no procedure has been provided in this Act the provisions of the Code shall apply.

36. **Order for payment of compensation**.-The Court 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 by commission of the offence 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 awarded:

Provided further that in connection with the powers under this section, the Court shall, apply the procedures as provided in the Code of Civil Procedure, 1908 (Act V of 1908).

37. **Qualifications for the Court**.-(1) Only a Court where the presiding judge has successfully completed training conducted by the Federal Judicial Academy with respect to all aspects of this Act including cyber forensics, electronic transactions and data protection shall be competent to hear any matter arising out of or in connection with this Act.

Provided that this section shall come into effect ninety days after the coming into force of this Act.

38. **Supply of statements and documents to the accused**.- (1) In all cases, copies of the entire investigation file, documents related to any proceeding or investigation and all evidence, including all exculpatory facts and evidence shall be supplied free of cost to the accused not later than fourteen days before the commencement of the trial:

Provided that the Court may direct that the cost of any storage devices required for supplying such copies may be paid by the accused in case the Court is satisfied that, for reasons to be recorded, the accused has access to such funds that would enable the accused to make such payment.

39. **Description of offence to be mentioned with specificity**.-The Court shall, when taking into consideration in a proceeding or mentioning any section of this Act in any document, including but not limited to any proceeding for issuance of warrant, bail, framing of charge or trial or any other proceeding with respect to or involving this Act, shall not merely consider and mention the section of the offence in question but shall also consider and specify the sub-section, clause and sub clause to identify exactly which offence is being referred to.

40. **Assistance to the Court**.-(1) The Court may be assisted in technical aspects by an *amicus curiae* having knowledge in *inter alia* all aspects of this Act including cyber forensics, electronic transactions and data protection and civil liberty safeguards with respect to exercise of procedural powers in cyberspace.

(2) The High Courts shall maintain a list of such *amicus curiae* having the relevant qualifications and experience.

(3) The Court shall also be assisted by the technical and forensic experts accredited by international organizations and approved by a joint committee of industry representatives and academicians.

(4) The Court shall determine the remuneration of the *amicus curiae* and the experts and may decide the party or parties to pay such remuneration, keeping in view the circumstances of each case.

(5) The investigating officer, prosecutor, complainant, victim or accused shall have the right to the appointment, presence and assistance of-

(a) amicus curiae

(b) technical experts; or

(c) forensic experts

at any stage of the case including but not limited to preliminary proceedings, bail hearing, acquittal hearing, framing of charge, trial or any other hearing.

41. **Preliminary assessment**.- (1) Upon the lodging of a report under section 155 of the Code, and again upon the filing of the interim investigation report under section 173 (1) of the Code, the

Court shall, without the need for any application for such preliminary assessment to be filed, no later than the following day make a preliminary assessment under subsections (2) and (3) respectively, as to whether an offence is made out against the accused and whether there is a likelihood of conviction based upon the facts placed on record and shall as the Court may deem appropriate:

(a) discharge the accused;

(b) if an accused is not in custody and:

(i) the case is of further enquiry, order that no arrests be made unless the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction; or

(ii) if the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction, proceed with the matter without prejudice to the right of any accused including his right to seek bail;

(c) if an accused is in custody and:

(i) the case is of further enquiry, order that the accused be released without bail subject to any future possibility of arrests if the Court is subsequently satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction; or

(ii) if the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction, proceed with the matter without prejudice to the right of any accused including his right to seek bail:

Provided that any assessment under this section shall only be tentative and shall be without prejudice to future determinations of the Court with respect to any further proceedings, including but not limited to bail, acquittal, framing of charge, or trial.

(2) The presence of the accused shall not be necessary for any proceeding, hearing or determination under this section.

42. **Right to anticipatory bail**.- (1) Any person whether an accused or apprehending that he may be arrested for a commission of an offence under this Act, whether or not nominated or named in any report under section 154, 155 or 173 of the Code shall have the right to seek bail and any court of competent jurisdiction shall have the power to grant him bail.

(2) Notwithstanding proceedings having taken place under subsection (1), any person whether an accused or apprehending that he may be arrested for a commission of an offence under this Act, whether or not nominated or named in any report under section 154, 155 or 173 of the Code shall have the right to move an application for another

preliminary proceeding under subsection (1) at any stage of the case whether during the stage of inquiry, investigation, trial, before judgment or in appeal.

43. **Anticipatory bail when person outside Pakistan.**- (1) When a person present outside the territorial limits of Pakistan comes to have knowledge of any circumstance under subsection (1) or (2) of section 42 and apprehends that he may be arrested upon his return to Pakistan for an offence under this Act, he shall have the right to seek bail or protective bail before any Court of competent jurisdiction without any need for his personal attendance and to be represented and appear by and through his pleader.

(2) The Court may at its discretion make such order as to provide such a person with assurance and protection on his return and secure his attendance according to such terms as it may deem fit.

(3) Should a person who has been granted bail under this section fails to return to Pakistan or abide by any of the terms thereof, the Court may cancel his bail and proclaim him an offender forthwith, ordering the investigating agency to take all measures through Interpol or mutual legal assistance treaties to secure the extradition and arrest of such person.

44. **Manner of recording evidence**.- For the purpose of recording evidence in all proceedings under this Act before a Court, the evidence of the witnesses shall be recorded in the following manner-

Entire Inquiry, Trial and all proceeding before the Court shall be video and audio recorded and copy of the same shall be made available to the accused directly or to his pleader as well as the prosecutor and the complainant directly or to his pleader by the close of the day of each proceeding:

Provided that no subsequent proceedings nor any order shall be issued by the Court related to the proceedings so recorded without first having provided a clearly viewable and audible copy of the video and audio recording to the accused directly or through his pleader at least three days before the next date of hearing or any subsequent proceeding in the case.

(2) The Court shall also cause a transcript of each proceedings to be prepared and provided to the accused directly or to his pleader as well as the prosecutor and the complainant directly or to his pleader no later than three days from the date of each proceeding or day before the next hearing, whichever is earlier.

45. **Appeal to High Court**.-Any person aggrieved by -

(a) any decision or order of the Court may prefer an appeal to the respective High Court within thirty days from the date of the decision or order of the Court:

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

CHAPTER V
MISCELLANEOUS

46. **Application of Electronic Transactions Ordinance, 2002**.-(1) Without prejudice to the application of the Electronic Transactions Ordinance, 2002 or any of its provisions, including subsection 2 of section 16 or clause (f) of subsection (1) of section 2 to the Electronic Transactions Ordinance, 2002 and any other law, the Federal Government may prescribe rules for communication, filing, submission or processing of any pleadings, evidence or documents by any person, including but not limited by or before the Court or by the investigating officer, the prosecutor, complainant or accused, with respect to any application or exercise of any power or provision under this law through electronic means or in electronic form.

(2) When prescribing rules for the application under subsection (1), the Federal Government shall have due regard to the availability, accessibility, security, authenticity and integrity of the electronic form or electronic means by which the enabling powers under sub-section (1) may be exercised by the Court, prosecutor, investigation agency or any other person.

Explanation: The Federal Government may, where it is appropriate in terms of the availability, accessibility and security, prescribe rules for the communicating, filing, submissions and processing of applications, pleadings and evidence and other documents in electronic form before the Court or by the prosecution, the investigation agency, complainant, accused or any other person. The use of these means would include instances such as electronic applications for any warrants; the supply of statements and documents to the accused; supply of evidence recorded; applying for a copy of seized data and other provisions under this law. However, the Federal Government shall ensure that such rules shall provide for the security, integrity and authenticity at all times of such means of communication, filing, submission and processing and only enable these means at locations where appropriate under the circumstances.

47. **Exclusion of telecommunication law related offences**.- (1) Nothing in this Act shall apply to any offence with respect to telecommunication or matters related to laws, or any subsequent amendment thereof, specified under the Schedule and vice versa.

(2) No offence in any law specified in the Schedule shall be included in or form the basis of any investigation, prosecution or trial before any Court related to any offence under this Act.

(3) Offences under laws specified under the Schedule shall be excluded from any investigation, prosecution, trial or exercise of powers conferred by, or operation of, any provision of this Act.

(4) Any investigating officer who exercises any power or attempts to exercise any power conferred by this Act or include offences specified under the First Schedule in any investigation, prosecution, trial or exercise of powers conferred by, or operation of, any provision of this Act, shall be subject to disciplinary action and shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to one million rupees or with both.

(5) No offence under this Act shall be included in or form the basis of any investigation, prosecution or trial before any Court related to any offence under this Act or any other law mentioned in the Schedule.

48. **Savings of Intelligence Services powers**.- (1) Offences, powers and procedures provided under this Act are not related to and have no application upon the activities, powers or functions of intelligence agencies or services and are without prejudice to the operation of or powers-

(a) under section 54 of the Pakistan Telecommunication (Re-organization) Act, 1996;
(b) under the Army Act, 1952;
(c) under the Air Force Act, 1953;
(d) under the Navy Ordinance, 1961;
(e) under the purview of the Intelligence Bureau;
(f) by the intelligence agency or intelligence service notified by the Federal Government under section 30 of this Act; and
(g) when exercised lawfully by any other intelligence agency or service that by itself does not investigate or prosecute an offence.

49. **Act to override other laws**.-The provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law and shall survive any amendment of any other law unless specifically amended or repealed.

50. **Power to amend Schedule**.-The Federal Government may, by notification in the official Gazette, amend the Schedule so as add any entry thereto but not omit any entry therein.

51**. Omission of section 36, 37 and inclusion of section 39, Ordinance LI of 2002**.-In the Electronic Transaction Ordinance, 2002 (LI of 2(02), sections 36 and 37 shall be omitted and section 39 shall be reinserted which shall read as follows:

"39. Prosecution and trial of offences.—No Court inferior to the Court of Sessions shall try any offence under this Ordinance."

THE FIRST SCHEDULE

{See sections 2(1)(s), 35, 47 and 50}

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

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

3. The Wireless Te1egraphy Act, 1933 (XVII of 1933).

_____
MAMNOON HUSSAIN,
President

_____
(_____),
Secretary

STATEMENT OF OBJECTS AND REASONS

Currently Pakistan has no comprehensive or even marginally adequate laws to 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 a completely new breed of cybercrime and criminals which cannot be combated with the use of existing 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 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 and invasive nature of the new powers that are necessary to investigate and prosecute these crimes requires their exercise to be proportionate with the civil liberty protections afforded citizens under the Constitution. This can only be achieved through strengthening existing protections and establishing new safeguards especially against abuse of these new and invasive 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 mitigate against Pakistan becoming a safe haven for cyber criminals but shall also contribute to the national security of the Nation whilst also providing an enabling and secure environment for investment in IT, E-commerce and E-payments and shall afford protection to

citizens which has hitherto been unavailable, exposing them to the unmitigated threats posed by cyber criminals both at home and abroad.