[TO BE INTRODUCED IN THE NATIONAL ASSEMBLY]

A

BILL

to make provisions for prevention of electronic crimes

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

It is hereby enacted as follows:--

1. **Short title, extent application and commencement.**- (1) This Act may be called the Prevention of Electronic Crimes Act, 2015.

(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 sub-clause (iii) of clause (b) 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 sub-clause (iv) of clause (b)—

(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, 1898 (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 sub-section (1) 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 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 in clause (o) of sub-section (1) of section (2) of the Electronic Transactions Ordinance, 2002 (LI of 2002);

(n) "information system" means information system as defined in clause (p) of sub-section (1) of section 2 of the Electronic Transactions Ordinance, 2002 (LI of 2002);

(o) "investigating officer" means an officer of the special investigation agency established under section 16;

(p) "negligence" means 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;

(za) "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

(zb) "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.

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 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