APPENDIX '1'

FINAL

"PREVENTION OF ELECTRONIC CRIME ACT"

INCLUSIVE OF ALL PROPOSED AMENDMENTS BY TREEQULAQ - READY FOR APPROVAL OF SENATE

ANNEX – B

[AS REPORTED BY THE STANDING COMMITTEE]

A

BILL

to make provisions for prevention of electronic crimes and matters related thereto

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

It is hereby enacted as follows: -

CHAPTER I
PRELIMINARY

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

(2) It extends to the whole of Pakistan.

(3) It shall apply to every citizen of Pakistan wherever he may be, and also to every other person, where ever he may be, who contravenes the provisions of this Act in any manner whatsoever which includes abetment, facilitation, conspiration or promotion.

(4) It shall come into force at once.

(5) It's not only limited to cyber offences only but encompasses any electronic crime committed on any e-Media.

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

(a) "act" includes_
i) a series of acts or omissions contrary to the provisions of this Act; or
ii) causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device, and whether having temporary or permanent impact;

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

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

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

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

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

(f) "authorised officer" means an officer of the investigation agency authorised to perform any function on behalf of the investigation agency by or under this Act. He or she will be compulsorily a Muslim if he or she has to deal with cases under Section 25 of this act;

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

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

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

(j) "critical infrastructure" includes:
(i) the infrastructure so vital to the State or other organs of the Constitution such that its incapacitation disrupts or adversely affects the national security, economy, public order, supplies, services, health, safety or matters incidental or related thereto or
(ii) any other private or Government infrastructure so designated by the Government as critical infrastructure as per rules prescribed under this Act;

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

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

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

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

(o) "device" includes-

(i) physical device or article;

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

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

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

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

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

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

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

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

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

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

(w) "minor" means, notwithstanding anything contained in any other law, any person who has not completed the age of following years.

(i) Boy: 12-15 years when gets nocturnal ejaculation or reaches 15 years without nocturnal ejaculation;
(ii) Girl: 9-12 years when gets menses or reaches 15 years without menses;

(x) "offence" means an offence punishable under this Act except when committed by a person who is not minor;

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

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

(aa) "service provider" includes a person who:

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

(ii) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services, such as PTCL, Ufone, Mobilink,Telenor, Zong, Warid etc; or

(iii) processes or stores data on behalf of such electronic communication service or users of such service, such as domain provider, host or any e-Space or e-Media owner, provider, admin etc or offices of facebook, google etc; or

(iv) provides premises from where or facilities through which the public in general may access an information system and the internet against payment of charges for the same such as cyber

cafes, Internet Service Providers, Cable Operators, relayers etc;

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

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

(dd)"unauthorised access" means access to such information system or data which is not available for access by general public, without without authorisation or in violation of the terms and conditions of the authorisation;

(ee) "unauthorised interception" shall mean in relation to an information system or data, any interception without authorisation;

(ff) "Non-Muslim" is the one who rejects Tauheed, Risalat, Finality of Prophet-Hood on Hadhrat Muhammad Mustafa ﷺ or any essential of Islam; including Dhimmi or Harbi, Ahle-Kitab like christians, jews or Non Ahle-Kitab, or atheist, infidel or polytheist like hindu, sikh or parsi or qaudiani or lahori (who call themselves ahmedi or any other name) or bahae etc (as per Article 260(3) and section 6 of the Constitution (Third) Amendment Order 1985 as incorporated by section 19 of the Constitution (Eighth) Amendment Act 1985);

(gg) "e-Space" It is electronic space or cyber space where people can upload, share, poll, sign petitions, comment, chat, place ads, make codes etc; including but not limited to websites, blogs, forums, pages, groups, domains, social media like facebook, cloud storage, video uploading sites like youtube, newsgroups, instant messaging, irc chatrooms, books uploaders, e-market places like amazon, education uploaders like wikipedia, mobile marketing services (like twitter 40404 service, pring, facebook sms updates, pring 9900, bulk sms etc) etc.

(hh) "e-Media" any electronic media or electronic device or information system, using any e-Space, including but not limited to; internet, computer, tablet, laptop, palmtop, watch, satellite, mobile, TV, cinema, cable, CDs, SIM, RIUM, hard disk, software, hardware etc or any future electronic device or electronic media or information system, not yet foreseeable.

(ii) "Online Data" any data placed or stored or uploaded or live streamed or broadcasting of recorded data; on internet, tv, cable etc including but not limited to; email, cloud storage, online drives, comments, videos etc, where access to data is possible by permitted users or audience, owner, uploader, host, domain owner etc;

(jj) "Offline Data" any data other than online data where access to data is possible by only owner of device etc, e.g., data stored in CD, DVD, Blue ray, Hard Disk, SIM, Memory card, mobile etc;

(a) "Derogatory Burning" includes burning only for e-blasphemous purposes, whether in the form of offline or online data, information, by depicting fire by offline software or online code etc;

(b) "Holy Personages" - عليهم الصلوة والسلام او رضوان الله عليهم اجمعين These include Last Holy Prophet Muhammad Mustafa ﷺ, other all Holy Prophets عليهم السلام, all Ahle Bait, all Sahabah رضوان الله عليهم اجمعين;

(c) "Holy Books and Manuscripts" Holy Quran, other 3 Holy Books, and Holy Manuscripts, if available in original form, may these be in book form or in the form of online or offline data;

(kk) "Holy Document" Any document which contains script about Allah عزوجل, Holy Books and Manuscripts, Holy Personages علیهم الصلوة والسلام و رضوان الله علیهم اجمعین, Holy Places etc, may it be in book form or in the form of online or offline data. Even comprising one word or phrase would be considered as document;

(ll) "e-Methods" any electronic methods; including but not limited to following:

(i) by words, either spoken e.g., remarks, videos or calls by skype, viber, whatsapp, line, voice chat, voice message, etc; or
(ii) by written words e.g., remarks, text, chat, email, sms, tweet, blasphemous code or script or program or function or game or software or any form of electronic custom application including mobile apps making, or android software, satirical comments, posts, polls, uploads, books, e-books, magazines, registering blasphemous domain or hosting etc; or
(iii) by visible representation like photo, video, picture, painting, drawing, cartoon, caricature, pornography, games, picture or video message, etc; or
(iv) by actions e.g., sharing, downloading, uploading, likes, tagging, place ads etc; or
(v) by celebrating or participating Charlie Hebdo event or 3 May Press Freedom day or 31 May Draw Muhammad ﷺday etc, may it be online or offline; or
(vi) by keeping online or offline e-blasphemous data especially of visible representation etc, just for the sake of knowledge, education, news, selling, buying etc; or
(vii) by serving in companies of websites etc involved in any kind of e-blasphemies; or
(viii) any information system owner or website owner or domain owner or host etc, not deleting e-blasphemous data etc of his own or of users or subscribers, or any service provider not filtering or blocking or removing such data; or
(ix) Desecrating or defiling or Derogatory Burning etc, any online or offline copy or any extract of Holy Books and Manuscripts or Holy Text or Holy Document etc, may these be in any format like pdf, word etc; or
(x) e-blaspheming using any crime or method mentioned in any provision of this act like including spamming, fraud, forgery, interception, spamming, cyber talking etc; or
(xi) by any other e-Methods or form of e-blasphemy not mentioned here but which may appear as outcome of new technology or inventions or innovations in softwares, programs, internet ideas, etc; or
(xii) by supporting or glorifying or facilitating or providing e-space to all above by: likes, comments, tweets, tags, posts, polls, sharing, downloading, uploading, signing petitions, polling, online or offline funds transfer, providing software, installing software, hosting, domain providing, etc; or supporting blacklisted ones, or putting data on any e-Media for education, news etc aimed at: supporting e-blasphemies, blasphemers or supporting to repeal blasphemy laws especially 295 C of chapter XV of Pakistan Penal Code 1860 (XLV of 1860) or by not deleting, blocking, removing any information of crime under section 25 of this Act, may he be any service provider, page admin, owner, domain provider etc;

(ff) "Abuse" it means insulting, making someone to do, supporting or glorifying or facilitating or only intending or planning to insult, with the following: including but not limited to: derogatory speech; or uttering derogatory comments or remarks; or deriding; or insulting just for amusement or mirthfully; or jesting, laughing, mocking, ludification, ridiculing; or laughing with or without blasphemers in support of their blasphemies; or humiliating, or defiling; or hate speech; or speak invective against; or

imputing; or to asperse with respect to religion; or to asperse with respect to Sacred Self or Holy Personality; or to asperse with respect to being Human or refer with malign the grievous happenings being Human; or to feel contempt about right or established grievous happenings being Human; or Defilement with respect to Parentage; or To asperse; or nagging; or abusing; or criticizing any of Holy Attributes; or pointing fingers or criticism or diatribe ; using diminutive noun; or belittlement; derision; lessening the Respect; performing and admitting an act based on hatred in heart; performing an act based on hatred in heart; or blaspheming or revilement; or accusing of lying or discrediting or refutation; or associate lie or false; or giving pain or troubling; or defiling speech or impertinent speech or uttering bad words; or Satirical speech or speaking ill of; or Speaking wrong or unreal of ; or Writing or singing satirical poems; or Obloquy by speech; or imprecating ; or curse; or seeking torment; or being ill wisher; or desiring harm; or vilify; or condemn; or referring Him ﷺ to His Sacred Related Things and Personalities in a vilifying manner; or associating something for purpose of condemnation; or annexing something absurd; or annexing something obscene; or annexing something bad; or discrediting referring to a distress or hardship which happened; or feeling boredom or displeasure towards Him- ﷺ; or any type of annoying contemptuously; sneer at or give an ugly grimace on listening Holy Name etc; or any form of faintest or slightest dishonor ; or vilifying on Might and Power or Eating; or vilifying on Self-Chosen Zuhd or Self-Chosen Faqr; or vilifying on Handsomeness and Adorableness; or saying that He ﷺfaced defeat or felt ashamed of; or complaining about Him ﷺ contemptuously; vilifying on Knowledge, Education, Prophetic Knowledge, Prophecy , or calling "Ummi" with mal-intention, or using word "uneducated" as depiction of word "Ummi"; or vilifying on Wisdom, Intellect, Comprehension; or reciting or using any Quranic Verse or Hadith Mubarakah with vilifying or derision intention about Him ﷺ; or not accepting Decision contemptuously; or a muslim considering , in heart, himself or herself or someone else than Holy Personages, equal or more pious than Holy Personages عليهم الصلوة و والسلام و رضوان الله عليهم اجمعين; or a muslim considering, anyone from Holy Personages عليهم السلام و رضوان الله عليهم اجمعين, equal or higher than Last Holy Prophet ﷺ; or a muslim considering, anyone who is not Prophet, equal or higher any Holy Prophet عليه الصلوة و والسلام; or calling with various Sacred Names or Sacred Patronymic Names; damaging or desecrating or Derogatory Burning an online or offline copy of the Holy Books or Manuscripts or any Holy Document or any extract therefrom, or placing them intentionally at derogatory place like filth dump etc or using them in any derogatory manner for any unlawful purpose; or narrating about Allah عزوجل , Holy Personages عليهم الصلوة و والسلام و رضوان الله عليهم اجمعين or Holy Books or Manuscripts or any Holy Documents or Holy Places at derogatory places; or interpreting any Sacred Text falsely from own side for insult; or raising voice in front of Him ﷺ ; or visiting Holy Grave in unclean or junub condition contemptuously; or talking badly about Anti Blasphemy Law (which is presently chapter XV especially 295-C of Pakistan Penal Code 1860 (XLV of 1860) and Judicial amendment of the Federal Shariat Court in 1990 and Sub-sections (2) to (9), especially (3) of Section 25 of this Act) or declaring it "black law" or uttering such like derogatory words for it or talking to repeal it or recommending such amendments in it which tend to reduce punishment; or vilifying on Holy Ismat; or insinuative insult or using defiling camouflaged dual meaning or ambiguous words; or using words resembling it or using resembling words for any insult written ante; or any other manner else than above written for reducing the Honour, etc;

(gg) "Defiling Manner" it includes but not limited to following; may it be: intentionally; or unintentionally; or due to lack of knowledge or ignorance; or not with deliberate or malicious intention of inciting or outraging or wounding the Muslims' feelings; or directly; or indirectly; or by habit; or seriously; or kiddingly or mirthfully; or hidden; or apparent; or Explicit ; or implicit; or by innuendo or hint or by oblique hints or by any gesture; or by allusive; or by insinuation; or by words, either spoken or

written; or by actions; or by visible representation; or by confession ; or by confession and insisting or pretending that his intention was otherwise; may it be proved by recurrence; or interpreting or narrating a blasphemous dream in a manner which disorientates the minds of people etc;

(hh) "e-Blasphemy or Cyber Blasphemy" is a cyber crime or electronic crime and e-terrorism or cyber terrorism, of highest level, committed by any person found Abusing; while using or creating or supporting or praising or facilitating etc any information or data, using any e-Methods or any Defiling Manner, against respect of Allah عزوجل , or any Holy Personages عليهم الصلوة و والسلام و رضوان الله عليهم اجمعين or Holy Books or Manuscripts or Holy Document or Holy Places;

(ff) "Essentials" it includes but not limited to following:- whether Muslim or Non-Muslim; and even if he does not confess or contradicts; and irrespective of man or woman; and may she be lactating or pregnant with pregnancy of less than 4 months 10 days; and if he/she is a minor then he/ she be jailed and asked on puberty, if he/ she still stays on blasphemy, then be given immediate punishment; and may he/she be President, Prime Minister, judge, ambassador etc; and immediate punishment; and if it is blasphemy against Prophet-Hood, then immediate punishment without giving respite for repentance and completion of prayer; and punishment without giving respite for completion of lactancy phase; and if pregnancy is less than 4 month 10 days, then punishment without giving respite for pregnant's delivery; and if pregnancy is more than 4 month 9 days, then be jailed and punishment immediately after delivery; and without giving respite for mensus or puerperium; and without any interpretations of Explicit; and if it is blasphemy against Prophet-Hood, then even if shows repentance before or after apprehension; and if it is blasphemy against Prophet-Hood, then regardless even if there exists witness for his/her repentance; and may he/she be drunken/ intoxicated or unconscious due to drinking; and may he/she be mad; and without declaring his/her heirs rightful of Qisas or Diyat; and even if he/she is near Holy Grave of Holy Prophet ﷺ or holding Holy Curtains of Holy Kaabah , or hidden inside Holy Kaabah, or inside any Masjid, be killed or punished there and then; and if he/she has Abused any Prophet عليہ الصلواۃ والسلام then; shall be punished by combing most of admonitory punishments including: amputation , mutilation , breaking teeth, burning, execution, crucification, by sword, by inserting dagger in belly even if she is pregnant or lactating, hanging 70 times or by suffocation, strafing with bullets, keep hanging for 1 day in public chowk, disheveling flesh pieces, tear into pieces, feasting him/her to vultures or dogs etc; and without giving chance of bail; and without hearing/ accepting mercy petition ; and no one including President is authorized to forgive; and without seeing intention; and without caring circumstantial presumptions; and if did not repent, then funeral shall neither be offered nor be bathed, coffined nor be buried in Muslim graveyard etc;

(gg) "Sacred Related Things" including but not limited to:

(i) Holy Grave (على صاحبهاالصلوةوالسلام) or Green Tomb (على صاحبهاالصلوةوالسلام) or Masjid Nabavi Shareef (على صاحبهاالصلوةوالسلام) or Hujrah Mubarakah or Riaz ul Jannah or Mimber Mubarak or Sacred Mawajahah etc or any of Sacred Belongings may they be Holy Swords, Holy Dresses, Holy Shoes etc or any other Sacred Related Things; of Our Beloved Last Holy Prophet Muhammad Mustafaa ﷺ; or

(ii) Any Holy Grave or Mausoleum etc or any of Sacred Belongings may they be Holy Swords, Holy Dresses, Holy Shoes etc or any other Sacred Related Things; of any other Holy Prophet عليہ السلام or Sahaabah رضوان الله عليهم اجمعين or other Holy Personalities رضوان الله عليهم اجمعين etc e.g., Maqam-e-Ibraheem عليہ السلام, Safa, Marwah, Holy Well of Zam Zam, The Ark of Covenant etc;

(hh) "Sacred Self" includes Sacred Personality, Holy Body may It be in Sacred Grave or Holy Part of

Holy Body like Cuttings of His Holy Nails or Holy Hair etc;

(d) Righteous Caliphs (Khulafa-e-Rashideen) رضوان الله عليهم اجمعين These include Hadhrat Abu Bkr Siddique, Hadhrat Umar Farooq, Hadhrat Usman Ghani, Hadhrat Ali AlMurtaza رضوان الله عليهم اجمعين respectively;

(ii) "Other Holy Sahaabah (Companions) or Holy Sahaabiyaat" رضوان الله عليهم اجمعين All Holy Sahaaba (Companions) or Holy Sahaabiyaat رضوان الله عليهم اجمعين except Righteous Parents, Members of the Sacred Families and Righteous Caliphs (Khulafa-e-Rashideen) رضوان الله عليهم اجمعين . These include but not limited to; Hadhrat Ameer Muavia, Hadhrat Abu Sufian, Hadhrat Habashi, Hadhrat Hindah (رضوان الله عليهم اجمعين) etc;

(jj) " Sacred Family (Ahle Bait)" it includes following Saahib e Iman Holy Personalities رضوان الله عليهم اجمعين:

(iii) Ancestry Sacred Family: Those Sacred Relatives who are because of Holy Father and Holy Grand Father e.g., Holy Maternal Uncle, Holy Paternal Uncle, Holy Paternal Aunt etc رضوان الله عليهم اجمعين; and

(iv) Home Sacred Family: Who settle in Sacred Home means Holy Wives رضوان الله عليهم اجمعين; and

(v) Birth Sacred Family: Holy Children born in Sacred Home including Holy Sons, Holy Daughters and their Holy Children onwards رضوان الله عليهم اجمعين; and

(vi) Declared Sacred Family: All those whom any Holy Prophet عليہ السلام declared them Part of His Sacred Family honorarily e.g., Hadhrat Salman Farsi رضوان الله عليهم اجمعين;

(kk) "Explicit" clear e-blasphemy, its interpretation will not be acceptable against convention and proverb.

(ll) Blacklist" means no appearance allowed for good, whether on ground or on any e-Media or on any e-Space, by permanent blocking access, removal, and providing data to investigating agency to trace elements behind. It includes blacklist of URLs or information and blacklist of Service Providers; for crimes under Section 25 and 34 of this Act. Blacklist of objectionable information and non-adherent Service Providers will be maintained by "Centre of Excellence for Information Management" and can be visible to Federal Government and its required part can be provided to Service Providers only for removal or blocking access;

(mm) "e-Treason" digging or supplying sensitive information against solidarity and integrity of Pakistan; to foreign hands, via any information system, e.g., digging or supplying secret information about softwares or methodology of censorship, sensitive installations, nuclear information, dispositions or deployments of Armed Forces, or disseminating secessionist or any other anti-state information, cyber snooping or cyber spying etc.

(nn) "FoRS - Freedom of Right Speech, FoRE - Freedom of Right Expression, FoRI - Freedom of Right Information, RoRP - Right to Right Rrivacy" in limits and light of Quran and Sunnah and Code.

(oo) "Terrorism" signifies the same definition as given in section 6 of ATA 1997;

(pp) "e-Terrorism" signifies the same definition as given in section 6 of ATA 1997, but on e-Media;

(qq) "Followers" if any Court or Federal Shariat Court or Mufti-e-barHaq, based upon proven facts or

evidences, convicts or declares a person to be blasphemer or e-blasphemer: then all persons who completely knew the decision of judge or verdict of Mufti, and were fighting for that blasphemer's case, including witnesses, advocates, lawyers, judges who gave decision in his support, bailers, mercy petitioners, signatories, friends of accused, and all persons who supported him like ulama who issued fatawa in his/ her favour, policemen who supported initiation of his case, persons involved in his exile or asylum, writers who wrote in his favour, speakers who spoke in his favour, or who made interpretations of Explicit in order to save e-blasphemer or to reduce his punishment or to hide his e-blasphemy, or saying a blasphemer not a blasphemer, all inclusive of judges, advocates etc who delayed punishment after finding requisite proofs, disciples of blasphemer, those who doubt his e-blasphemy or punishment, etc, catering Essentials, will be considered blasphemers or e-blasphemers, and will be named as "Followers".

(rr) "Assisting Organization" Any private, Pro-Pakistan, free of sectarianism, Islamic organization, if willing to assist and cooperate with Authority by providing authenticated, URLs or information: of Anti-Islam or of crimes under Sub-sections (2) to (8) and (12) of Section 25 of this Act, or of Anti-State or Anti-Armed forces, along with analysis, scrutiny and justification; then that organization may be designated as "Assisting Organization" and registered with Authority[1].

(2) Unless context provides otherwise, any other expression used in this Act or rules framed thereunder but not defined in the Act, shall have meanings assigned to the expression in the Pakistan Penal Code, 1860 (XLV of 1860), the Code of Criminal Procedure, 1898 (V of 1898) and the Qanoon-e-Shahadat Order, 1984 (X of 1984), as the case may be.

CHAPTER II
OFFENCES AND PUNISHMENTS

3. Unauthorised access to information system or data.- Whoever intentionally gains unauthorised access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine up to one fifty thousand rupees or with both.

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

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

6. Unauthorised access to critical infrastructure information system or data:- Whoever intentionally gains unauthorised access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine up to one million rupees or with both.

[1] Justification: In this way long checking channel to confirm whether link is blasphemous or otherwise, will be not required/ cut short due to support of that assisting organization, being trustworthy enough to send legitimate anti-Islam links free of sectarianism.

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

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

9. Glorification of an offence and hate speech. Whoever prepares or disseminates information, through any information system or device, where the commission or threat is with the intent to:-

(a) glorify an offence under any law for the time being enforced in Pakistan or the person accused or convicted of a crime; or
(b) support terrorism or activities of proscribed organizations; or
(c) advance religious, ethnic or sectarian hatred;

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

Explanation: "Glorification" includes depiction of any form of praise or celebration in a desirable manner.

10. Cyber terrorism. –Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9 of this Act, where the commission or threat is with the intent to:-

(a) 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 create a sense of fear or insecurity in society; or

(b) advance religious, ethnic or sectarian discord,

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

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

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

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

13. Making, obtaining, or supplying device for use in offence.- Whoever intentionally produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, primarily to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to 6 months or with fine up to fifty thousand rupees or with both in addition to punishment of specific crime under respective section of this Act.

14. Unauthorised use of identity information.-(1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorisation shall be punished with imprisonment for a term which may extend to three years or with fine up to five million rupees, or with both.
(2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.

15. Unauthroised issuance of SIM cards etc.- Whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or other portable memory chip designed to be used in cellular mobile or wireless phone for transmitting information without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine up to five hundred thousand rupees or both.

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

Explanation: A "unique device identifier" is an electronic equipment identifier which is unique to a mobile or wireless communication device.

17. Unauthorised interception.- Whoever intentionally commits unauthorised interception by technical means of:-

(a) any transmission that is not intended to be and is not open to the public, from or within an information system; or
(b) electromagnetic emissions from an information system that are carrying data,

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

18. Offences against dignity of natural person- (1) Whoever intentionally publicly exhibits or displays or transmits any false information, which is likely to harm or intimidate the reputation or privacy of a natural person shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both:

Provided, nothing under this sub-section (1) shall apply to anything aired by a broadcast media or distribution service licensed under Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for passing of such orders for removal, destruction or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application, may take such measures as deemed appropriate for securing, destroying, blocking access or preventing transmission of such information.

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

a) superimposes a photograph of the face of a natural person over any sexually explicit image; or
b) distorts the face of a natural person or includes a photograph or a video of a natural person in sexually explicit conduct; or
c) intimidates a natural person with any sexual act,

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

(2) Whoever commits an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term which may extend to one year, or with fine up to one million rupees or with both.

(3) Any grieved person or his guardian, where such person is a minor, may apply to the Authority for passing of such orders for removal, destruction or blocking access to such information referred to in sub-section (1) and (2) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying, blocking access or preventing transmission of such information.

20. Malicious code.- Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine up to one million rupees or both.

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

21. Cyber stalking.- (1) Whoever with the intent to coerce or intimidate or harass any person uses information system, information system network, the Internet, website, electronic mail, information or any other similar means of communication to:-

(a) communicate obscene, vulgar, contemptuous, or indecent information; or
(b) make any suggestion or proposal of an obscene nature; or
(c) threaten to commit any illegal or immoral act; or
(d) take a picture or photograph of any person and display or distribute without his consent or knowledge in a manner that harms a person**;** or
(e) display or distribute information in a manner that substantially increases the risk of harm or violence to any person;

commits the offence of cyber stalking.

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

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

(3) Any aggrieved person may apply to the Authority for issuance of appropriate orders for removal or destruction of, or blocking access to such information as referred to in sub-section (1) and the Authority upon receipt of such application may take such measures as deemed appropriate for removal or destruction of, or blocking access to, such information.

22. Spamming.- (1) Whoever intentionally transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without the express permission of the recipient, or causes any information system to show any such information commits the offence of spamming.

Explanation.- "Unsolicited information" does not include:

i. Marketing authorized under the law; or
ii. Information which has not been specifically unsubscribed by the recipient.

(2) A person engaged in direct marketing shall provide the option to the recipient of direct marketing to block or subscribe such marketing.

(3) Whoever commits the offence of spamming as described in sub-section (1) or engages in direct marketing in violation of sub-section (2), for the first time, shall be punished with fine not exceeding fifty thousand rupees and for every subsequent violation shall be punished with imprisonment for a term which may extend to three months or with fine up to one million rupees or with both.

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

(2) Whoever commits spoofing shall be punished with imprisonment for a term which may extend to three years, or with fine up to five hundred thousand rupees or with both.

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

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

25. Pakistan Penal Code 1860 to apply:- (1) The provisions of the Pakistan Penal Code 1860 (XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act.

(2) "Any person who is found committing e-Blasphemy, against respect of following; he/ she along with Followers shall be declared apostates (in case they were muslims) and Allah's blasphemers, and if he/ she and any Followers persist even after given 3 days repentance time; then he/ she along with his/ her persistent

Followers, catering Essentials, would be immediately punished only with death penalty:

(a) The Holy Essence or any of Divine Attributes or any of Sacred Names of Allah Almighty etc; or

(b) Any of Sacred Names or any Copy of the Holy Qur'an or of any extract therefrom (as present in 295-B of chapter XV of Pakistan Penal Code 1860 (XLV of 1860)); or

(a) Any of Sacred Names or a Copy of any other 3 Holy Books or any of Holy Manuscripts or of any extracts therefrom, if available in original form; or

(3) "Any person; if found committing e-Blasphemy, against respect of following; then he/ she along with Followers, shall be declared apostates (in case they were muslims) and Prophet's blasphemers and punished immediately, catering Essentials, only with death penalty:

(a) Sacred Self, or any of Sacred Names or Religion or any of Sacred Attributes or Uswah Hasanah or Sacred Mannerism or any of Sacred Ahadith-e-Mutawatrah Mashhura Khbr Wahid or any Sacred Sunnah or any of Sacred Related Things or Holy Company or Sacred Condition etc of Our Beloved Last Holy Prophet Muhammad Mustafaa ﷺ (under 295-C of chapter XV of Pakistan Penal Code 1860 (XLV of 1860) and Judicial amendment of the Federal Shariat Court in 1990); or

(b) Sacred Self or any of Sacred Names or Religion or any of Sacred Attributes or Uswah Hasanah or Sacred Mannerism or any of Sacred Sayings which is Mutawatrah Mashhura Khbr Wahid or any of Sacred Sunnah or any of Sacred Related Things or Holy Company or Sacred Condition etc of any other Holy Prophet علیہ السلام;

(4) "Any person; who is found committing e-Blasphemy, against respect of Sacred Self, or any of Sacred Names, or Religion, or any of Sacred Character Traits, or any of Mutawatrah Mashhura Sacred Sayings, or any of Sacred Doings or any of Sacred Related Things or Holy Company or Sacred Condition etc of following; he/ she along with Followers shall be declared Ahle Bait's or Sahaba's blasphemers and if he/ she and any Followers persist even after given 3 days repentance time; then he/ she along with his/ her persistent Followers, would be immediately punished, catering Essentials, with quantity of lashes equal to 100:

(a) Any of Righteous Parents (رضوان اللہ علیہم اجمعین), of the Last Holy Prophet (ﷺ); or

(b) Any of the Righteous Caliphs (Khulafa-e-Rashideen رضوان اللہ علیہم اجمعین) , of the Last Holy Prophet (ﷺ); or

(c) Any of the Members of the Sacred Family (Ahle-Bait) of the Last Holy Prophet (ﷺ) including His Holy Wives (Ummahatul Mumineen) رضوان اللہ علیہم اجمعین except Hadhrat Aysha رضی اللہ عنہا; or

(d) Any of Other Holy Sahaaba (Companions) or Holy Sahabiyaat رضوان اللہ علیہم اجمعین , of the Holy Prophet (ﷺ); or

(e) Any of Righteous Parents (رضوان اللہ علیہم اجمعین), of any other Holy Prophet علیہ السلام; or

(f) Any of the Members of the Sacred Families of any other Holy Prophet علیہ السلامincluding His Holy Wives رضوان اللہ علیہم اجمعین; or

(g) Any of other Holy Sahaaba (Companions) or Holy Sahabiyaat رضوان اللہ علیہم اجمعین , of any other

Holy Prophet علیہ السلام;

(5) "Any person; who is found committing e-Blasphemy, against respect of Sacred Self, or any of Sacred Names, or Religion, or Holy Ismat, or any of Sacred Character Traits, or any of Mutawatrah Mashhura Sacred Sayings, or any of Sacred Doings or any of Sacred Related Things or Holy Company or Sacred Condition etc of Hadhrat Aysha Siddiqah رضی اللہ عنہا ; he/ she along with Followers shall be declared apostates (in case they were muslims) and Allah's blasphemers, and if he/ she and any Followers persist even after given 3 days repentance time; then he/ she along with his/ her persistent Followers, catering Essentials, would be punished immediately with death penalty.

(6) "Any person: who is found committing e-Blasphemy, or destroys or damages, using any e-Media, against respect of following; if he/ she and any Followers persist even after given 3 days repentance time; then he/ she along with his/ her Followers, catering Essentials, would be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both (under 295 of chapter XV of Pakistan Penal Code 1860 (XLV of 1860)) and with other such strongest punishment, which must be decided unanimously:

(a) Holy Kaabah Musharrafah; or

(b) Masjid Haram; or

(c) Any other Masjid;

(7) Quadiani group or the Lahori group (who call themselves 'Ahmadis' or by any other name), or Followers of Yusuf Kazzab (including Zaid Zaman etc), Ismaeli, Bohry, Agha Khani or any other Non-Muslim or any other group for whom the Federal Shariat Court declares that its beliefs are against Islam; involved in:

(a) Misuse of epithets, descriptions or titles, etc., reserved for certain Holy Personages علیہم الصلوۃ والسلام و رضوان اللہ علیہم اجمعین or Places; or

(b) refers to the mode or form of call to prayers followed by his faith as "Azan", or recites Azan as used by the Muslims; or

(c) who poses himself as a Muslim, or calls, or refers to, his faith as Islam, or preaches or propagates his faith, or invites others to accept his faith, or makes his worship places on pattern of Masajid; or

(d) Outrages, in any manner whatsoever, the religious feelings of Muslims

directly or indirectly, using any e-Methods, on any e-Medium, shall be punished with imprisonment of either description for a term which may extend to three years, and with fine, (under 298-B and 298-C of chapter XV of Pakistan Penal Code 1860 (XLV of 1860)) and access to their websites or links or any local or foreign presence on e-Media or by using any e-Method, will be blocked immediately by Authority.

(8) Anyone, using any e-Media, talking badly about Anti Blasphemy Law for Sanctity of Prophet-Hood (which is presently 295-C of chapter XV of Pakistan Penal Code 1860 (XLV of 1860) and Judicial amendment of the Federal Shariat Court in 1990 and Sub-section (3) of Section 25 of this Act) or declaring it "black law" or uttering such like derogatory words for it or talking to repeal it or recommending such amendments in it which tend to reduce punishment, catering Essentials, would be declared blasphemer or e-blasphemer of Prophet-Hood and be immediately punished along with his Followers, with only death penalty.

(9) Any Muslim; using any e-Media, refutes any of essentials of Islam or accepts other religion; if persists even after given 3 days repentance time; then he/ she would be punished with death penalty after declaring apostate.

(10) Anyone; may be after losing control on himself/ herself or under grave or sudden provocation; who kills someone extra judiciously, claiming charge of blasphemy or e-blasphemy committed by the murdered one in respect of Last Holy Prophey Muhammad Mustafa ﷺ or any other Holy Prophet علیہ السلام , if;

1) he/ she can prove, based on evidence, said blasphemy or e-blasphemy committed by the murdered one; or

2) he/ she is unable to produce evidence but any Islamic Scholar (Alim or Mufti), before or after the murder, gives verdict declaring blasphemer for said blasphemy or e-blasphemy committed by the murdered one; or

3) Any court or Federal Shariat Court; based upon proven facts or evidences, has already convicted the murdered one, before murder or thereafter declares blasphemer, for said blasphemy or e-blasphemy;

then, he/ she shall be clear i.e., he/ she shall neither be given any punishment nor shall he/ she be subject to Qisas nor shall he/ she be kept in imprisonment for investigation.

(11) Only Muslim Judge shall give decision about blasphemy or e-blasphemy.

(12) Anybody found committing e-Treason, shall punishable with death penalty and that organization shall be blacklisted.

26. Other Offences:- Any offence under any Law for the time being enforced in Pakistan, if committed, promoted, facilitated using, any information system, shall apply to the offences provided in this Act.

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

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

(2) Unless otherwise provided for under this Act, the investigation agency, the authorised officer 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.

(3) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science, detection, tracing and tracking techniques (for locating webhost, domain providers, admins, Unique Identifiers, Identity Information, account IDs, IP addresses etc and decryption etc) and hiring law or security institutions trained technical persons and other related matters for training of the officers and staff of the investigation agency.

(4) Investigating agency shall also investigate elements (e.g., through any techniques to trace unique identifiers, IDs, IP addresses etc or by decryption etc) behind the anti-Islam, anti-Pakistan and anti-Armed forces URLs or information on any e-Medium, originating from anywhere, especially from Pakistan.

28. Power to investigate.- Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act:

Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams comprising of the authorised officer of investigation agency and any other law enforcement agency for investigation of offence under this Act and any other law for the time being in force.

29. Establishment of "Special Emergency Anti-Blasphemy Shariat Court" under Federal Shariat Court:-

(1**)** A regular "Special Emergency Anti-Blasphemy Shariat Court" be established under Federal Shariat Court for hearing and decision of all blasphemy cases including e-blasphemy cases under Sub-Sections (2) to (10) of Section 25 of this Act, for immediate evidence collection on emergency basis, while the accused will be kept in Anti Terrorist prison and investigated by investigation agency and authorized officer. After getting evidences or recurrence**Error! Bookmark not defined.** or accused confesses that he wrote or spoke Explicit words[2] or when such court is satisfied, convict will be served with punishment as per respective provision, immediately in timeframe not exceeding 1 hour**Error! Bookmark not defined.**. Federal Government is bound to prescribe rules for this purpose.

(2**)** Nobody; including President, Prime Minister etc, will have the right to repeal, challenge, appeal or amend punishment of convicted blasphemer after decision of "Special Emergency Anti-Blasphemy Shariat Court" under Federal Shariat Court.

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

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

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

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

Provided that the authorized officer shall immediately but not later than twenty four hours bring to the notice of the Court, the fact of acquisition of such data and the court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise.
(2) The period provided in sub-section (1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorised officer in this behalf.

[2] Justification:- This point is in accordance with Purifying Shariah Law as per old Scholars of Islam (Reference 4, Appendix 'A').

31. Retention of traffic data:- (1) A service provider shall, within its existing or required technical capability, retain its traffic data for a minimum period of one year or such period as the Authority may notify from time to time and provide that data to the investigation agency or the authorised officer whenever so required.

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

(3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to six months or with fine up to five hundred thousand rupees or with both.

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

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

(b) has been acquired by a person as a result of the commission of an offence,

the Court may issue a warrant which shall authorise an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data or other articles relevant to the offence identified in the application.

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

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

33. Warrant for disclosure of content data:- (1) Upon an application by an authroised 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 an offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system or data, to provide such data or access to such data to the authorised officer.

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

34. Powers of an authorised officer.-(1) Subject to provisions of this Act, an authorised officer shall have the powers to -

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

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

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

(d) have access to or demand any information, 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 authorised officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person;

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

(g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence:

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

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

(a) act with proportionality;

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

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

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

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

(3) When seizing or securing any information system or data, the authroised officer shall make all efforts to

use technical measures while maintaining its integrity and chain of custody and shall only seize an information system, data, device or articles, in part or in whole, 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.

35. Dealing with seized data:- The Federal Government may prescribe rules for search and seizure and dealing with the information system, data or other articles searched and seized under this Act.

36. Power to manage online information.- (1) The Authority is empowered to manage information and issue directions for removal or "blocking of access" of any information through any information system.
The Authority or any officer authorised by it in this behalf may direct any service provider, to remove any information or block access to such information, if it/ he/ she considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or to harness pornography, drug trafficking, e-smuggling, overseas online gambling, or in relation to contempt of court, or commission of or in support of or incitement to an offence under this Act.

(2) The Authority may prescribe rules for adoption of standards and procedure to manage information, block access and entertain complaints.

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

(4) Authority may establish a dedicated unit while allocating funds and human resources, supported by state of art technical solutions and upgraded call center, named "Centre of Excellence for Information Management"; with the mandate to respond to any threat or attacks and to take requisite measures by proactively and independently detecting, providing data to investigating agency to trace elements behind, blacklisting, blocking access and removing; the websites or blogs or URLs or any information on any information system or on any e-Media, both local or foreign but visible in Pakistan, may it be of any NGO, involved or in support of:

(i) Crimes under Sub-Sections (2) to (8) of Section 25 of this Act; and

(ii) Anti-State and anti-Armed Forces Propaganda; and

(iii) Miscellaneous; e.g., Pornographic, Drug trafficking, e-Gambling etc;

(5) "Centre of Excellence for Information Management" shall have Computer Emergency Response Teams for above three purposes, headed by a liaison officer. These will block access and remove information by: using any firewall, blocking technique including open blocking or silent blocking or filtering technique including PC-based and android based filtering, or hacking, using any equipment or software as deemed appropriate or by issuing directions to Service Providers. "Centre of Excellence for Information Management" will work as one window operation; i.e., objectionable URLs or information, can be submitted by any citizen of Pakistan at this centralized location at prescribed phone number and email attended to 24 x 7. Objectionable URLs or information so received or detected, their access shall be immediately blocked temporarily on emergency basis, before scrutiny, in time not exceeding 15 minutes and shall be later scrutinized, in time not exceeding 6 hours, for subsequent decision of its blacklisting.

(6) Federal Government may formulate electronic or cyber security strategy to cater cyber or electronic spying

by foreign secret agencies and may establish "Electronic or Cyber security Task Force" for counter measures to proactively combat cyber warfare and cyber aggression and to counter propaganda attacks, which will work under umbrella of "Centre of Excellence for Information Management".

(7) Computer Emergency Response Teams, under "Centre of Excellence for Information Management", responsible for crimes under Sub-sections (2) to (8) of Section 25 of this Act; shall also have an "Islamic Scholars Panel" duly qualified by Federal Shariat Court. Objectionable URLs or information detected or received, will be scrutinized in time not exceeding 6 hours, by "Islamic Scholars Panel" or responsibility of scrutinizing may be designated to other body; e.g., to "Assisting Organization". After scrutiny, access to blacklisted URLs or information, shall remain blocked on permanent basis and removed within period not exceeding 24 hours.

(8) Computer Emergency Response Teams under "Centre of Excellence for Information Management", responsible to counter crimes of Anti-State and anti-Armed Forces Propaganda my designate responsibility of scrutinizing anti-Pakistan and anti-Armed forces URLs or information to ISPR or ISI as "Assisting Organization".

(9) "Assisting Organization" for crimes under Sub-sections (2) to (8) of Section 25 of this Act will be designated after approval by Federal Shariat Court. It shall receive URLs or information of crimes under Sub-sections (2) to (8) of Section 25 and may detect such content at its own in addition and shall submit such content back, via fastest means, duly scrutinized by its own "Islamic Scholars Panel" within stipulated timeframe. To build trust, Authority and Federal Shariat Court may monitor and verify authenticity of URLs or information submitted by Assisting Organization, initially for few times. In return to its assistance, Authority shall respond quickly according to URL or information submission schedule, mutually agreed upon via MoU. URLs or information submitted by Assisting Organization will be immediately attended to by liaison officer especially URLs or Information having e-blasphemy against Holy Prophet ﷺ.

(10) Service Providers non-adherent, within stipulated timeframe, to the instructions of "Centre of Excellence for Managing Information", may be considered supporter of that crime and may be punished under respective section under this Act and their licenses will be cancelled. Non-adherent Service Providers shall be included in blacklist for lifetime banning and further prosecution under that section of Act along with fine not less than 5000000.

(11) If any child URL or information, involved or in support of, crimes under Sub-sections (2) to (8) of Section 25 of this Act, has been written or put or uploaded etc by Service Provider or website owner etc on any e-Space or e-Media, then that Service Provider or website owner etc will be blacklisted for life time removal and blocking access of that Parent URL or blog or website along with all other blogs or websites or information of same author or website owner or Service Provider.

(12) If any child URL or information, involved or in support of, crimes under Sub-sections (2) to (8) of Section 25 of this Act, has been put or uploaded by any user etc of Service Provider or website owner etc on any e-Space or e-Media, and if such child URL or information cannot be removed or its access cannot be blocked by Authority due to any unavoidable reason; then access to Parent URL or whole website or blog will be blocked within stipulated timeframe and will remain blocked till the time not a single objectionable information related to crimes under under Sub-sections (2) to (8) of Section 25 of this Act, is visible or available on any child URLs of that Parent URL or website or blog, in any region of Pakistan. Prior to unblocking Parent URL or whole website or blog, "Islamic Scholars Panel" of "Centre of Excellence for Information Management" will render a certificate to this effect, or responsibility may be designated to assisting organization: that no traces of objectionable information or Parent or Child URLs of crimes under

Sub-sections (2) to (8) of Section 25 of this Act, are left. If after unblocking of access, crime under under Sub-sections (2) to (8) of Section 25 of this Act, is repeated, then Service Provider or website owner etc will be blacklisted for life time removal and blocking access of that Parent URL or blog or website along with all other blogs or websites or information of same author or website owner or Service Provider..

(13) Blacklisted information or URLs or Service Providers or NGOs will be continuously surveilled not to appear in another form or name or unique identifier or site, by "Centre of Excellence for Information Management". Their bank accounts shall be seized and sources of funding, may it be online, shall be stopped for good by investigating agency.

(14) If the submitted objectionable URL or information of crime under Section 25 or 34 of this Act, has not been removed or blocked its access within stipulated timeframe, by Authority or "Centre of Excellence for Information Management", then submitter reserves right to appeal and Authority is liable to answer.

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

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

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

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

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

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

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

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

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

Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days.
(2) Notwithstanding anything contained in any law to the contrary the information so collected under sub-section (1) shall be admissible in evidence.

(3) The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorises an extension for a further specified period.

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

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

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

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

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

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

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

(f) 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.

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

CHAPTER IV
INTERNATIONAL COOPERATION

40. International cooperation.-(1) The Federal Government may on receipt of request, extend such cooperation to any foreign Government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act.

(2) The Federal Government may, at its own, forward to a foreign Government, 24 x 7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other Government, agency or organization etc., as the case be in initiating or carrying out investigations or proceedings concerning any offence.

(3) The Federal Government may require the foreign Government, 24 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 Federal Government may send and answer requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

(5) The Federal Government may refuse to accede to any request made by a foreign Government, 24 x 7 network, any foreign agency or any international organization or agency if the request concerns an offence which may prejudice its national interests including its sovereignty, security, public order or an ongoing investigation or trial.

(6) Any NGO found involved or in support of crime under Sub-sections (2) to (8) of Section 25 of this Act or under Section 34 of this Act; would be blacklisted, both in Pakistan and internationally, by seeking International Cooperation may be via Interpol or UN, along with respective punishments under respective Sub-Sections of Section 25 of this Act.

(7) Pakistani blacklist about crimes under Sub-sections (2) to (8) of Section 25 of this Act shall be shared, by Federal Government, with other Islamic countries. Govt. Federal Government to stress upon Islamic World to share e-blasphemous information held with one Islamic country, with all Islamic countries may be through platform of OIC or OIC-Computer Emergency Response Team or other Muslim Computer Emergency Response Teams etc for immediate blocking access or removal or joint pursual of elements behind, for global and united prevention of e-blasphemous crimes.

(8) Federal Government to stress upon Islamic World, by using platform of OIC, to form one combined core United Islamic Internet System, own search engines, video and content sharing social media etc, constantly

monitored for e-blasphemous content by one unanimous Joint Blocking And Filtration Setup, adequately equipped, manned and funded by all Islamic countries.

(9) Information or data acquired by investigating agencies and "Centre of Excellence for Information Management" about whereabouts of blacklisted ones (behind information or Service Providers etc), may be shared, by Federal Government with Interpol, or UN etc for tracing purposes or for global and united prevention of electronic crimes.

(10) Federal Government to continuously stress upon international media and UNO through platform of OIC etc, for formulation and acceptance of "Inter-Religion Law of Mutual Sustenance" of respecting Holy Prophets (عليهم الصلوة والسلام) and death penalty to blasphemers of all Holy Prophets (عليهم الصلوة والسلام) and advocate as torch bearer of FoRS - Freedom of Right Speech, FoRE - Freedom of Right Expression, FoRI - Freedom of Right Information, RoRP - Right to Right Rrivacy etc.

CHAPTER – V
PROSECUTION AND TRIAL OF OFFENCES

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

Provided that offences under section 15 shall be cognizable by the investigation agency on a written complaint by the Authority.
(2) Offences under section 10 and 19 and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency.

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

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

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

(4) To the extent not inconsistent with this Act, the procedure laid down under the Code of Criminal Procedure 1898 (V of 1898) and the Qanoon-e-Shahadat Order 1984 (X of 1984) shall be followed.

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

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

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

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

CHAPTER VI
PREVENTIVE MEASURES

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

(2) Any owner of the information system or service provider who violates the guidelines issued by the Federal Government under sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine upto ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both.

47. Computer Emergency Response Teams:- (1) The Federal Government may formulate one or more Computer Emergency Response Teams or designate any assisting organization; to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan or attacks on Islam or Pakistan or Armed Forces.
(2) A Computer Emergency Response Team constituted under sub-section (1) may comprise of technical experts of known expertise, officers of any intelligence agency or any sub-set thereof, may be duly foreign trained. Team may initially hire foreign professional technial staff e.g., content removal experts, blocking access experts, censor or filter experts and hackers for subsequent ToT (Transfer of Technology).

(3) A Computer Emergency Response Team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed.

CHAPTER VII
MISCELLANEOUS

48. Relation of the Act with other laws:- (1) The provisions of this Act shall have effect not in derogation of the Pakistan Penal Code, 1860 (XLV of 1860), the Code of Criminal Procedure, 1898 (V of 1898) and the Qanoon-e-Shahadat Order, 1984 (X of 1984), the Protection of Pakistan Act, 2014 (X of 2014) and Investigation for Fair Trial Act, 2013 (I of 2013).

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

(3) The provisions of this Act shall override the provisions of Chapter XV of Pakistan Penal Code 1860 (XLV of 1860).

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

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

(a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors;
(b) powers, functions and responsibilities of the investigation agency, its officers and prosecutors;
(c) standard operating procedures of the investigation and prosecution agency;
(d) mode and manner in which record of investigation under this Act may be maintained;
(e) manner to deal with the seized data, information system, device or other articles;
(f) working of joint investigation teams;
(g) requirements for seeking permission of the Authority to change, alter or re-program unique device identifier of any communication equipment by any person for research or any other legitimate purpose;
(h) procedure for seeking appropriate orders of the Authority for removal, destruction or blocking access to information under this Act;
(i) constitution of Computer Emergency Response Team and the standard operation procedure to be adopted by such team;
(j) appointment of designated agency having capability to collect real time information;
(k) manner of coordination between the investigation agency and other law enforcement and intelligence agencies including designated agency;
(l) for management and oversight of the forensic laboratory;
(m) qualifications and trainings of the officers, experts and staff of the forensic laboratory;
(n) powers, functions and responsibilities of the forensic laboratory, its officers, experts and staff;
(o) standard operating procedures of the forensic laboratory to interact with the investigation and prosecution agency;
(p) manner of soliciting and extending international cooperation, and
(q) matters connected or ancillary thereto.

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

51. Amendment of Electronic Transactions Ordinance, 2002 (LI of 2002) and pending proceedings:- (1) Sections 36 and 37 of the Electronic Transactions Ordinance, 2002 (LI of 2002) are omitted.
(2) Any action taken by or with the approval of the authority or proceedings pending under the provisions of the Electronic Transactions Ordinance, 2002 (LI of 2002) repealed by sub-section (1), shall continue and be so deemed to have been taken or initiated under this Act.

52. Savings of powers:- Nothing in this Act shall affect, limit or prejudice the duly authorized and lawful powers and functions of the State institutions performed in good faith.

STATEMENT OF OBJECTS AND REASONS

Currently Pakistan has no law to comprehensively deal with the growing threat of cybercrime. The centuries old criminal justice legal framework is inadequate and ill equipped to address the sophisticated online threats of the 21st Century cyber age. While this new age has exacerbated existing crimes when conducted with the use of the Internet/ any other electronic media, which are adequately addressed by the application of the Electronic Transactions Ordinance, 2002 in conjunction with existing criminal justice legislation, it has also given birth to completely new types of cybercrime and criminals which cannot be effectively dealt with through the use of 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 of individuals/organizations in the virtual world. The legislation therefore, establishes new offences including illegal access of data (hacking), as well as interference with data and information systems (DOS and DDOS attacks), specialized cyber related electronic forgery and electronic fraud, cyber terrorism (electronic or cyber attack on the critical information infrastructure), unauthorized interception conducted by civilians, use of malicious code, viruses, identity theft etc.

The legislation provides new investigative powers hitherto unavailable such as search and seizure of digital forensic evidence using technological means, production orders for electronic evidence, electronic evidence preservation orders, partial disclosure of traffic data, real time collection of data under certain circumstances and other enabling powers which are necessary to effectively investigate cyber crime cases. The very technical nature of the new powers that are necessary to investigate and prosecute these crimes require their exercise to be proportionate with the civil liberty protections afforded to citizens under the Constitution. This can only be achieved through strengthening existing protections and establishing new safeguards especially against abuse of these new and intrusive powers. The Bill also includes specific safeguards to balance against these intrusive and extensive procedural powers in order to protect the privacy of citizens and avoid abuse of the exercise of these powers.

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

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