Analysis on Prevention of Electronic Crimes Bill 2016

	Government's Bill	Proposed Amendments	Justification
	PREAMBLE		
	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:	An Act to make provisions for securing electronic material against unauthorized access, transmission or modification, and cyber fraud and for connected purposes.	
	Chapter 1: PRELIMINARY		
1	**Short title, extent, application and commencement.-** (1) This Act may be called the Prevention of Electronic Crimes Act, 2016.		

	(2) It extends to the whole of Pakistan. (3) It shall apply to every citizen of Pakistan wherever he may be and also to every other person for the time being in Pakistan. (4) **It shall also apply to any act committed outside Pakistan by any person if the act constitutes an offence under this Act and affects a person, property, information system or data located in Pakistan."** (5) It shall come into force at once.	**OMIT**	This would allow the law to be applied to foreigners without providing any process or mechanism. For certain crimes mentioned it may be important to add the "foreign aspect" but this can not be applied in its entirety.
2	**Definitions**	**Definitions**	For definitions, refer to the Budapest Convention and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
	(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;	(a)	
	(c) "access to information" means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;	(b)	
	(d) "Authority" means the Pakistan Telecommunication Authority established under	**(c) OMIT**	

	the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);		
	(e) "authorization" means authorization by law or the person empowered to make such authorization under the law: Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;	(d) "Authorization" means authorisation by law or the person empowered to make such authorisation under the law; (e)	
	(f) "authorized officer" means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;	(f) "Authorised officer" means an officer of the designated investigation agency authorised to perform any function on behalf of the investigation agency by or under this Act;	
	(g) "Code" means the Code of Criminal Procedure, 1898	(g) "Code" means the Code of Criminal Procedure, 1898 (V of 1898);	

	(Act V of 1898);		
	(h) "content data" means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;	(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;	(i) "Court" means the Court of Sessions competent to try offenses, issue warrants and pass orders under this Act;	
	(j) "critical infrastructure" **means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in:** **i. major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant**	(j)	

	loss of life or casualties – taking into account significant economic or social impacts; or ii. **significant impact on national security, national defense, or the functioning of the state".** **Provided that the Government may designate any private or Government infrastructure as critical infrastructure as may be prescribed under this Act.**		
	(k) "damage to an information system" means any unauthorized change in the ordinary working of an information system that impairs its performance,	(k) "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	

	access, output or change in location whether temporary or permanent and with or without causing any change in the system;	location whether temporary or permanent and with or without causing any change in the system;	
	(l) "data" includes content data or traffic data;	(l) "data" includes content data and traffic data;	
	(m) "data damage" means alteration, deletion, deterioration, erasure, relocation, suppression of data or making data temporarily or permanently unavailable;	(m) "data damage" means alteration, deletion, deterioration, erasure, relocation, suppression, of data or making data temporarily or permanently unavailable;	
	(n) "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,	(n) "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	

	programs or information systems;	information systems;	
	(o) "dishonest intention" means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred ***"or incitement to violence"*** ;	Malicious intent needs to be added. Despite the addition of "incitement of violence"	
	(p) "electronic" includes electrical digital, magnetic, optical, biometric, electrochemical, electromechanical , wireless or electromagnetic technology;	(o) "electronic" includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology;	
		(p) "fraudulently" shall have the meaning assigned to it in section 25 of the Pakistan Penal Code, 1860.	
		(q) "Government" means the Federal Government.	
	(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) "identity information" means information, in any form whatsoever, whether presently existing or which may emerge in future with the advent of modern devices and technology, used alone or in combination with other information, which may authenticate or identify an individual or an information system and enable	See PECB'14 as approved by the Cabinet Division Refer to definition (l)

		access to any data or information system;	
	(s) "information" includes text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) and codes including object code and source code;	(t) "information" includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;	
	(t) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;	(u) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;	
	(u) "integrity" means in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or	(v) "integrity" means, in relation 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	

	advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;	particular point in time;	
	(v) "interference with information system of data" means and includes an unauthorized act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data;	(w) "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.	
	(w) "investigation agency" means the law enforcement agency established by or designated under this Act;	(x) "investigation agency" means the law enforcement agency established by or designated under this Act;	
	(x) "minor" means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years;	(y) "minor" means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years.	
	(y) "offence" means an offence punishable under this Act except when committed by a person under ten years of age or	(z) "offence" means an offence punishable under this Act;	See Section 299a of the PPC See Article 10 (b) of the ICCPR

	by a person above ten years of age and under fourteen years of age, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion;		
	(aa) "rules" means rules made under this Act;	(aa) "rules" means rules made under this Act;	
	(bb) "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;	(bb) "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;	
	(cc) "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,	(cc) "service rovider" includes a person who: i. acts as a service provider or intermediary 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	See definition in Budapest Convention

	possesses, operates manages or controls a public switched network or provides telecommunication services; or iii. possesses or stores data on behalf of such electronic communication service or users of such service;	provides telecommunication services; or iii. processes or stores data on behalf of electronic communication service providers mentioned in (i) and (ii) above or users of such electronic communication service.	
	(dd) "subscriber information" means any information held in any form by a service provider relating to a subscriber other than traffic data;	(dd) "subscriber information" means any information held in any form by a service provider relating to a subscriber other than traffic.- data;	
	(ee) "traffic data" includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;	(ee) "traffic data" includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;	
	(ff) "unauthorized access" means access to an information system or data which is not available for access by general public, without authorization or in violation of the	(ff) "unauthorised access" means deliberate access to an information system or data without i. legal right or authorisation and in disregard for absence of such legal right or authorization, or	See definitions (y) & (z) PECB'14 as approved by the Cabinet Division See definition in Budapest Convention

	terms and conditions of the authorization;	ii. in violation of the terms and conditions of the authorization granted by the person entitled to grant such authorization.	
	(gg) "unauthorized interception" shall mean in relation to an information system or data, any interception without authorization; and	(gg) "unauthorized interception'' shall mean in relation to an information system or data, any deliberate interception without legal right or authorization;	
	(hh) "unsolicited information" means the information which is sent for commercial and marketing purposes against explicit rejection of the recipient and does not include marketing authorized under the law.		
	(2) Unless the context provides otherwise, any other expression used in this Act or rules made thereunder but not defined in this Act, shall have the same meanings assigned to the expressions in the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898) and the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), as the case may be.	3. 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	**Unauthorized access to information to system or data.-** Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.	**Unauthorised access to information system or data.-** Whoever with malicious intent gains unauthorised access to any information system or data shall be punished with fine up to one fifty thousand rupees or with both.	The word "intentionally" has been replaced with "with dishonest intention" in **Sections 3, 4, 5, 6, 7, 8, 9 and 17**. In Section 23 "dishonestly" has been replaced with "with dishonest intention." It was earlier recommended "malicious intent" be added to all clauses. What needs to be discussed further is what "dishonest intention" constitutes and its place in existing jurisprudence, whether is adequate as mens rea or should be replaced with "malicious intent" as was earlier suggested. With regards to Sections 3,4, 6 & 7, their potential to be misapplied to whistleblowers and journalists remains a huge concern. In an environment where even though freedom of information is recognized by the Constitution and legislation to enable access to it exists, the culture is still to deny information and exclusionary clauses are cited more often than not, to ensure it is not shared. Leaked information is how the whistle is blown on a lot of overreach by governments, their organizations and others. While information must surely not be used to blackmail intimidate or scandalize people, however
4	**Unauthorized copying or transmission of data.-** Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both.	**Unauthorised copying or transmission of data.-** Whoever with malicious intent and without authorisation accesses and copies or otherwise transmits or causes to be transmitted any data shall be punished with fine up to one hundred thousand rupees or with both.	
5	**Interference with information system or data.-** Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.	**Interference with information system or data.-** Whoever with malicious intent interferes with and/or damages or causes to be interfered with or damage 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	**Unauthorized access to critical infrastructure**	**Unauthorised access to critical infrastructure information system or data:-**	

	information system or data.- Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.	Whoever with malicious intent 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.	certain information only finds it way into the public domain when it is leaked and someone blows the whistle on it. The right balance must be struck which cannot be done by changing the language of this alone but ensuring that enabling legislation with protections for data, whistleblowing etc are in place to draw from. For whistleblower protection see NADRA whistle-blower system, Khyber Pakhtunkhwa's right to information law and the Federal Board of Revenue (FBR) is seeking to do the same through the Finance Act 2015 See Principles 16-18 Johannesburg Principles
7	**Unauthorized copying or transmission of critical infrastructure data.-** Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both.	**Unauthorised copying or transmission of critical infrastructure data.-** Whoever with malicious intent and without authorisation copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall he 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 with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data , shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both.	**Interference with critical infrastructure information system or data.-** Whoever with malicious intent interferes with or damages, or causes to be interfered with or damage, 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** Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence	**Incitement, Glorification of terrorism** Whoever with malicious intent prepares or disseminates information, through any information system or device to:-	The major contentions in this clause are: 1. "the intent to glorify an offence and the person convicted of a

	"relating to terrorism; or any" convicted of a crime relating to terrorism or activities of proscribed organizations "***or individuals or groups***" shall be punished with imprisonment for a term which may extend to **"seven years"** or with fine which may extend to ten million rupees or with both. ***Explanation.-*** "glorification" includes depiction of any form of praise or celebration in a desirable manner.	a) incite an act of terror; b) glorify and 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.	crime relating to terrorism" remains. What of those accused and held under the Anti-Terrorism Act: the I-11 protestors or those in Okara. Individuals and groups campaigning for the release of those wrongly booked of crimes, advocating for the quashing of cases etc could be charged on the pretext of glorifying the alleged offence or person, even though it is an appeal for justice and due process. 153-A of the PPC and 11W of the Anti Terrorism Act, both cover this. See Article 10 (a) of the ICCPR See Principles 1, 2, 6, 7, 8 and 23 of the Johannesburg Principles See OSCE Joint Statement See: ECHR case Jersild v Denmark (and Article 19's note) See GNI report on Extremist Content and the ICT Sector 2. The penalty has been increased from 5 to 7 years which is harsh considering the above mentioned issues with the language.

			See UNESCO report on "Countering Hate Speech Online"
10	**Cyber terrorism.** Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to__ (a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance inter-faith, sectarian or ethnic hatred, **(c) Advance the objectives of organizations, individuals or groups proscribed under the law.** **10-A. Hate speech.- Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance inter-faith, sectarian or ethnic hatred, shall be punished with imprisonment for a term which may extend to seven**	**Cyber terrorism.-** Whoever with malicious intent commits or attempts to commit any of the offences under sections 6, 7 and 8 of this Act, where the commission or attempt is 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. **10 A: OMIT**	The word "religious" in (b) has been replaced with "inter-faith" and "discord" with "hatred." The word "overawe" has been removed. This section carries a jail term of fourteen years and a fine of up to fifty million rupees. The language is incredibly vague and this is a cognizable offence How this will be determined is not clear. While this applies in relation to Sections 6,7, 8 and 9, chances are, people will either be booked under both sections or the higher penalty will be invoked. This is a cognizable offence which non-bailable and non-compoundable. See Principle 22 Johannesburg Principles See Necessary & Proportionate Principles on Proportionality 10 A: Newly added provision describing hate speech is vague and doesn't define hate speech. Also a repetition of the section 11-W under ATA. Should be deleted.

	years or with fine or with both. **10-B. Recruitment, funding and planning of terrorism.- Whoever prepares or disseminates information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plans for terrorism shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.** shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.		
11	**Electronic forgery.-** (1) Whoever interferes with or uses any information system, device or data, with the intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with	**Electronic forgery.-** 1) Whoever with malicious intent for wrongful gain 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	See Articles 7 and 8 of the Budapest Convention Read here a paper on Computer-related fraud and Identity Fraud by a Professor from the Faculty of law at the University of Verona

	property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to two hundred and fifty thousand rupees or with both. (2) Whoever commits offence under sub-section (1) in relation to a critical infrastructure information system or data shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to five million rupees or with both.	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 both with. 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 the intent for wrongful gain interferes with or uses any information	**Electronic fraud:-** Whoever with malicious intent for wrongful gain interferes with or uses any information system,	

	system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.	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 produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to six months or with fine which may extend to fifty thousand rupees or with both.	**Making, obtaining, or supplying device for use in offence.-** Whoever with malicious intent produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, 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.	
14	**Unauthorized use of identity information.-** (1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment	**Unauthorized use of identity information.-** 1) Whoever with malicious intent, fraudulently obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with	Refer to California Criminal Law: Unauthorized use of Personal Identifying Information Read here a paper on Computer-related fraud and Identity Fraud by a Professor from the Faculty of law at the University of Verona

	for a term which may extend to three years or with fine which may extend to five million rupees, or with both. (2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.	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 wrongfully 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 due and reasonable measures to protect the best interest of the aggrieved person for securing, destroying or preventing transmission of such identity information, pursuant to the provisions of this Act. 3) The Authority shall make bylaws for carrying out purposes referred to in sub-section (2) pursuant to provisions of this Act.	
15	**Unauthorized 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 ***"universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless***	**15. Un Unauthorized issuance of SIM cards etc.-** Whoever with **malicious intent** 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 ***"universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices such as tablets,"***	Both offences are already covered under Pakistan Telecommunication (Re-organisation) Act, 1996 - see Section 31 on offences and penalties See Section 47: Exclusion of telecommunication related offences PECB'14 as approved by the Cabinet Division

	phone or other digital devices such as tablets," 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 which may extend to five hundred thousand rupees or with both.	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 authorization changes, alters, tampers with or re- programs unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving information shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both. ***Explanation.__*** A "unique device identifier" is an electronic equipment identifier which is unique to a mobile wireless communication device.	**16. Tampering etc. of communication equipment.-** Whoever with malicious intent or without authorization of the Authority 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 Intelligence shall be punished with imprisonment which may extend to three years or with fine up to one million rupees or both; Provided that the Authority shall frame bylaws under the provisions of this Act to enable persons, including individuals, companies and research organizations, to seek prior permission from the Authority to change, alter or re-program unique device identifier of any communication equipment for any legitimate purpose. ***Explanation:*** A "unique device identifier" is an electronic	

		equipment identifier which is unique to a mobile wireless communication device.	
17	**Unauthorized interception.-** Whoever with dishonest intention commits unauthorized interception by technical means of__ (a) any transmission that is not intended to be and is not open to the public, from or within an information system; or (b) electromagnetic emissions from an information system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.	**17. Unauthorized interception:-** Whoever with malicious intent commits unauthorized interception by technical means of:- a) any electronic transmission that is not intended to be and is not open to the public from or within an information System, or b) electro magnetic 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 and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which	**Offences against dignity of natural person**.- 1) When a person with malicious intent through an information system, a) produces, offers and makes available, distributes or transmits, procures or solicits, or possesses sexually explicit images of a natural person, or b) produces, offers and makes available, distributes or transmits, procures or solicits or possesses an image, photograph or	18. "which he knows to be false" has been added and "likely to" before "harm to reputation" has been omitted. This section criminalizes the act of exhibiting, displaying or transmitting information a person "knows to be false" that "harms or intimidate the reputation or privacy of a natural person." This carries a jail term of up to three years and a fine up to one million rupees. While this doesn't apply to anything aired on television, it applies to everything uploaded and shared online.

	may extend to one million rupees or with both: Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinanc e, 2002 (XIII of 2002). (2) Any aggrieved person or his guardian, where such person is a minor, "***shall forthwith***" apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application, may pass such orders as deemed *"**reasonable in the circumstances"*** including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.	video of a natural person in sexually explicit conduct or intimidates or threatens a natural person with production, distribution or transmission of such material, or **c)** cultivates, entices or induces a minor to engage in a sexually explicit act or in a lewd manner that is offensive to the privacy of the minor,shall be punished with imprisonment for a term up to three years which may extend up to six years in relation to a minor or with fine up to ten million rupees or both. 2) **<u>Anyone, including the guardian</u>** of the aggrieved 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 due and reasonable measures to protect the best interest of the aggrieved person for securing, destroying or preventing transmission of such information, pursuant to the provisions of this Act. 3) The Authority shall make bylaws for carrying out purposes referred to in sub-section (2) pursuant	Political expression and satire is not exempted. Some examples how this can be misapplied: The person who uploaded Rehman Malik's video of boarding a flight late would be jailed for it. In fact he did lose his job and was charged under the Maintenance of Public Order. PTI activist Qazi Jalal was charged under Section 36 & 37 of the ETO for a tweet in which he alleged a judge's son-in-law was deriving benefits due to his in-laws' position. He included a wedding card in his tweet to corroborate the person in question was actually the son-in-law. In Turkey, a man is facing a two-year jail term for sharing a meme comparing Erdogan and Gollum – character from the Lord Of The Rings Trilogy. Would the same happen to person who created/shared the Nawaz Sharif & Shrek meme? And any other form of political expression, satire or citizen journalism will be construed as harm to reputation. Either people will start to self-censor – as is now rampant on channels and do a great degree in print – or people will have FIRs lodged against them and face jail terms. We already have defamation laws and there is no need to criminalize defamation. The following addition has been made to Sections 19 and 21: "and the Authority

		to provisions of this Act.	may also direct any of its licensees to secure such information including traffic data." What the practices to secure such information are not defined. Securing traffic data under this Act does not require a warrant. In the Philippines, the real- time collection of traffic data clause in their cybercrime law was struck down by the Supreme Court in 2014 Technology activists were successful in making their case before court that even traffic data was identifiable data and therefore its collection infringed privacy and opened doors to mass surveillance. In the absence of data protection and privacy legislation, this cannot be left up to the discretion of an executive authority. Already Sections 18, 19 and 21 allow the 'aggrieved' to apply directly to the PTA for 'removal or destruction of, or blocking access of such information' 'the Authority on receipt of such application, may pass such orders as deemed appropriate including an order for removal, destruction of, or blocking access to, such information.' Section 18 is already covered under Defamation Ordinance 2002 and Defamation (Amendment) Act 2004 and penalized under Section 500 and 501 of the PPC.

			Section 19 is partly covered under Section 509 of the PPC and can be further amended to make it gender neutral and more specific. For Section 21 see Sections 503, 506 and 507 of the PPC. See Lahore High Court's interim order in the 'YouTube case,' BytesforAll vs Federation of Pakistan, and submissions made by PTA, Google and independent experts Read Islamabad High Court's order (a modified version of this initial order) in Bolo Bhi vs Federation, challenging the PTA and government's power to block content online See Indian Supreme Court's judgment striking down 66a of the Indian IT Act See Manila Principles i.e. II Content must not be required to be restricted without an order by a judicial authority See: Hate Crimes in Cyberspace by Danielle Citron, a professor at the University of Maryland's Francis King Carey School of Law. See Chapters 3, 5 and 6 of the UNESCO Report on Fostering Freedom Online: The Role of Intermediaries
19	**Offences against modesty of a natural person and**		"or video" has been added to sub section (a)

	minor.- (1) Whoever intentionally and publicly exhibits or displays or transmits any information which– (a) superimposes a photograph of the face of a natural person over any sexually explicit image or video; or (b) Includes a photograph or a video of a natural person in sexually explicit conduct; or (c) intimidate a natural person with any sexual act or any sexually explicit image or video of a natural person; or (d) cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to **"five"** years or with fine which may extend to five million rupees or with both. (2) Whoever commits an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term which may extend		"or any sexually explicit image or video of a natural person" added to (c) new sub section (d) has been added which reads "cultivates, entices or induces a natural person to engage in a sexually explicit act" with the following addition after it: "through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail." The offence if committed with respect to a minor, carries a jail term and fine, whereas previously it was imprisonment or fine.

	to **"seven years"** and with fine which may extend to **"five"** million rupees: Provided that in case of a person who has been previously convicted of an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term of "**"ten"** years and with fine. (3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, may shall forthwith pass such orders as deemed appropriate reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.		

20	**Malicious code.-** Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or with both. ***Explanation.-*** For the purpose of this section, the expression "malicious code" includes, a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorization.	**20. Malicious code.-** Whoever with malicious intent 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) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, website, electronic mail or any other similar means of		The language has been slightly altered. Sub sections (a)-(c) have been replaced with new clauses. The addition of "make a video" has been made to (d) (d) can have wide connotations. What about pictures taken without permission if they are covering crowds at public

	communication to– (a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; (b) monitor the use by a person of the Internet, electronic mail, text message or any other form of electronic communication; (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or (d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person. (2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment for a term which may extend to one year or with fine which may extend to one million rupees or with both:		events? Or those pictures zeroing in on public/known figures attending rallies/congregations by banned organizations, in an attempt to call them out or hold them accountable for it? This carries a jail term of up to three years. Again, it is not court but the PTA to whom the 'aggrieved" party can apply just like Sections 18 and 19. And the following addition has been made to this section too: "and the Authority may also direct any of its licensees to secure such information including traffic data."

	Provided that if victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to five years or with fine which may extend to ten million rupees or with both. (3) Any aggrieved person or his guardian, where such person is a minor, ***"shall forthwith"*** apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, may pass such orders as ***"reasonable in the circumstances"*** appropriate including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.		
22	**Spamming.-** (1) A person commits the offence of spamming, who with intent	**20. Spamming.-** 1) Whoever with malicious intent transmits unsolicited information in bulk repeatedly to any	The definition of spamming is incredibly vague. This section criminalizes the transmission of "has been criminalized. It is unclear as

	transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain. (2) A person including an institution or an organization engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing. (3) Whoever commits the offence of spamming as described in sub-section (1) ***by transmitting harmful, fraudulent, misleading or illegal or engages in direct marketing in violation of sub-section (2), for the first time, information, 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 three months***	recipient who has expressly unsubscribed from receiving such bulk information, commits the offence of spamming. ***Explanation:-*** "Unsolicited information in bulk" does not include (i) marketing authorized under the law, or (ii) information that 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.	to how one should acquire permission. This will disrupt the very nature of public messaging relied on not only by businesses and political parties, but rights defenders and entrepreneurs. There is no need to include such a provision in a criminal law, or criminalize the act. There are other ways of dealing with this, particularly through the existing telecommunications regulatory regime or, through tools available in mobile phones and email inboxes. People should not be jailed for what is an irritant. Examples of Spam Acts in other countries: Australia: Spam Act 2003 USA: CAN-SPAM Act of 2003 Singapore: Spam Control Act 2007 Canada: Anti-Spam Legislation 2014 Read this on the Canadian Anti-Spam Law See Indian Supreme Court's judgment striking down 66a of the Indian IT Act that allowed people to be arrested for 'annoying' or 'offensive' content.'

	or with fine which may extend to one million rupees or with both" (4) Whoever commits the offence of spamming as described in sub-section (1) by transmitting unsolicited information, or engages in direct marketing in violation of sub-section (2), for the first time, shall be punished with fine not exceeding to fifty thousand rupees, and for every subsequent violation shall be punished with fine not less than fifty thousand rupees that may extend up to one million rupees.		
23	**Spoofing.-** (1) Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing. (2) Whoever commits spoofing shall be punished with imprisonment for a term which may extend to three years or with fine which		See Articles 4: Right not be tried or punished twice of Protocol No.7 to Convention for the Protection of Human Rights and Fundamental Freedoms

	may extend to five hundred thousand rupees or with both.		
24	**Legal recognition of offences committed in relation to information system.-** (1) Notwithstanding anything contained in any other law for the time being in force, an offence under this Act or any other law shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to or through the use of an information system. (2) References to "property" in any law creating an offence in relation to or concerning property, shall include information system and data.	**24. Legal recognition of offences committed in relation to information system.-** 1) Notwithstanding anything contained in any other law for the time being in force, an offence under this Act or any other law shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to, or through the use of an information system. 2) References to "property" in any law creating an offence in relation to or concerning property, shall include information system and data.	
25	**Pakistan Penal Code, 1860 (Act XLV of 1860) to apply.-** The provisions of the Pakistan Penal Code, 1860 (Act XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act.	**25. Pakistan Penal Code 1860 to apply.-** 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.	

CHAPTER III ESTABLISHMENT OF INVESTIGATION AGENCY AND PROCEDURAL POWERS FOR INVESTIGATION			
26	**Establishment of investigation agency.-** (1) The Federal Government may establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act. (2) Unless otherwise provided for under this Act, the investigation agency and the authorized officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act. (3) The investigation agency shall establish its own capacity for forensic analysis of the data or information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency.	**26. Establishment of investigation agency.-** 1) The Federal Government shall establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act. 2) Unless otherwise provided for under this Act, the investigation agency and the authorised officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act. **3) OMIT** 4) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency, and all authorized officers exercising powers or performing functions pursuant to this Act shall have received prior training in digital	See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See Necessary & Proportionate Principles on Integrity of Communications & Systems & Safeguards against Illegitimate Access and Right to Effective Remedy (3) Clause 26 (3) new addition should be deleted. Forensic lab should be independent of any Authorised agency as mentioned in the previous draft in sec 37. This newly inserted provision is not only giving powers to agency to generate forensic reports but also making it mandatory for courts to admit the reports as evidence

	(4) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency.	forensics, information technology or computer science, in such terms as may be prescribed.	
27	**Power to investigate.-** Only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act: Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams comprising of an authorized officer of the investigation agency and any other law enforcement agency for investigation of an offence under this Act and any other law for the time being in force.	**27. No warrant, arrest, search, seizure or other power not provided for in the Act.-** Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act and no search and seizure of information or system or arrest of person shall be affected except upon grant of warrant by the Court: Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams headed by the authorised officer of the designated investigation agency and comprising officers of any other law enforcement agency for investigation of offence pursuant to the provisions of this Act.	Section 54-A CrPC (as amended) requires the person being arrested to be informed of the grounds of the arrest. See Section 17 of PECB'14 as approved by the Cabinet Division See Articles 9, 14, 15 & 17 of the ICCPR See Principle 20 and 24 of the Johannesburg Principles
28	**Expedited preservation**	**28. Expedited preservation of**	An 'authorized officer' may write to a person in control

	and acquisition of data.- (1) If an authorised officer is satisfied that- (a) ***"specific"*** data stored in any information system or by means of an information system is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the authorized officer may, by written notice given to the person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice: Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of acquisition of such data and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case	**data.-** 1) Upon an application by an authorized officer that demonstrates to the satisfaction of the Court that- a) ***"specific"*** data stored in any information system or by means of an information system, is reasonably required for the purposes of a criminal investigation; and b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the Court may, by written notice given to a person in control of the information system, require that person 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: 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. 3) The person in control of the information system shall only be responsible to preserve the data specified- a) for the period of the preservation and maintenance of integrity specified in	of an information system and require him/her to provide data or order that specified data be preserved up to 90 days. It is after this is done that the authorized officer must bring this to the court's attention within 24 hours. So post-PECB, we will be receiving written orders from not even the agency but an officer, to hand over data. 24 hours is long enough a period to misuse the powers given. See Section 18 (2) and (3) of PECB'14 as approved by the Cabinet Division See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See Necessary & Proportionate Principles on Proportionality, Competent Judicial Authority, Public Oversight, Integrity of Communications & Systems See clause 55 in David Kaye's report under Anonymity

	including issuance of warrants for retention of such data or otherwise. (2) The period provided in sub-section (1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorized officer in this behalf.	the notice or for any extended period permitted by the Court; and b) where it is technically and practically possible to preserve the data and maintain its integrity. 4) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, 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.	
29	**Retention of traffic data.-** (1) A service provider shall, within its ***"specified"*** existing or required technical capability, retain its	**29. Retention of traffic data.-** 1) A service provider shall, within its existing technical capability, retain its traffic data up to a period of 90 days or such	a service provider (i.e. ISP) is required to retain data (of its customers) up to a year and provide it to the investigation agency or authorized officer as and when notified by the

	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 "**subject to production of a warrant issued by the court,"**or the authorized officer whenever so required. (2) The service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transactions Ordinance, 2002 (LI of 2002). (3) Any owner of the information system who is not a licensee of the Authority and violates sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both:	lesser period as the Authority may notify from time to time and provide such traffic data to the designated investigation agency "**subject to production of a warrant issued by the court,"** or the authorised officer pursuant to provisions of Section 30. 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).	Authority to do so. Our entire digital footprint – what we accessed, who we communicated with and the specific contents – would be on offer. Also, retention of data is quite costly and this will be an added expense for service providers. Clause 29:The amendments have added judicial oversight over handling the data to the authorised officer although we have recommended to decrease the data retention period from 1 year to 3 months. See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See clause 55 in David Kaye's report under Anonymity See Necessary & Proportionate Principles - specifically Integrity of Communications & Systems See Manila Principles V (e) about intermediaries and disclosure of identifiable information Philippines Supreme Court struck down this provision from their cybercrime law in 2014. Technology experts argued traffic data was identifiable data and therefore infringed privacy and opened doors to mass surveillance.

	Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the license and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996. (Act.____of 1996)		
30	**Warrant for search or seizure.-** (1) Upon an application by an authorized officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that- (a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an	**30. 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 storage medium of a specified kind 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 after recording reasons issue a warrant which shall authorise an officer of the designated investigation agency, with such assistance as may be necessary to enter in the presence of a judicial magistrate	See Section 19: Warrant for Search and Seizure PECB'14 as approved by the Cabinet Division

	offence, the Court may issue a warrant which shall authorize an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offence identified in the application. (2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted officer of the investigation agency, may enter the specified place and search the premises and any information system, data, device or other articles relevant to the offence and access, seize or similarly	the specified place and to search the specified premises and specified information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure the specified information system, data or other articles relevant to the offence identified in the application. 2) The application under subsection (1) shall in addition to substantive grounds and reasons also: a) explain why it is believed the material sought will be found on the premises to be searched; and b) why the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them; 3) No court shall issue any warrant to enter and search any specific premises, information system, data, device or other articles, unless satisfied that consequent upon the particulars of the offence referred to in the application, there are reasonable grounds for believing that it is necessary to search the specific premises, information system, data, device or other articles in order to find the material sought.	

	secure any information system, data, device or other articles relevant to the offence: Provided that the authorized officer shall immediately but not later than twenty-four hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.		
31	**Warrant for disclosure of content data.-** (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that the person in control of the data or information system, to provide	**31. Warrant for disclosure of traffic data.-** 1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that 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 traffic data, to disclose sufficient traffic data about a specified communication to identify-	This section pertains to the 'disclosure of content data.' It speaks nothing of data other than content data. In this bill, data is defined as 'traffic data and content data.' Moreover other forms of 'data' are covered under other definitions. Information for instance is defined as: 'text, message, data, voice, sound, database, video, signals, software, computer programs, any form of intelligence as defined under the PTA (Reorganization Act 1996 and codes including object code and source code.' So while a warrant would be required for disclosure of 'content data,' there is no procedure nor oversight prescribed for the acquisition, disclosure, retention, preservation or

	such data or access to such data to the authorized officer. (2) The period of a warrant issued under sub-section (1) may be extended beyond seven days if, on an application, a Court authorizes an extension for a further period of time as may be specified by the Court.	a) the service providers; and b) the path through which provide such traffic data or access to such traffic data to the authorised officer. 2) The period of a warrant issued under sub-section (1) may be extended if, on an application, a Court authorises an extension for a further period of time as may be specified by the Court. 3) The application under sub-section (1) shall in addition to substantive grounds and reasons also explain why it is believed the traffic data sought will be available with the person in control of the information system. **31. Warrant for acquisition of information or data other than traffic data.-** 1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that 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 disclose sufficient data about a specified	handling of traffic data – which is also identifiable data (i.e. can reveal a person's location, identity and more. Nor does this exist for information – the definition for which contains nearly all forms of data. Moreover Section 31 deals with a person in control of the information system or data, and not service providers or those storing data on behalf of others. Therefore the token warrant for content data hardly serves as a safeguard for the above-listed sections, which give sweeping powers over - and intrusive access - to everyone's communication and data. And there is no data protection or privacy legislation in Pakistan. See Section 20: Warrant for for disclosure of traffic data PECB'14 as approved by the Cabinet Division

		communication to identify- 2) The application under sub-section (1) shall in addition to substantive grounds and reasons also explain why it is believed the data sought will be available with the person in control of the information system. **31. Warrants for arrest.-** 1) No person shall be arrested or detained with respect to or in connection with any offence under this Act unless a warrant for arrest has been issued by the Court under this section. 2) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that a specified person identified in the application has committed or participated in the commission of an offence under this Act, the Court may, after recording reasons, issue a warrant which shall authorise an authorized officer, with such assistance as may be necessary, to arrest the person identified in the application. 3) The application under sub-section (1) shall in addition to substantive grounds and reasons also explain why it is reasonably believed that the person identified in the application committed or participated in the	

		commission of an offence under this Act. 4) No court shall issue any warrant to arrest any person unless satisfied that consequent upon the particulars of the offence referred to in the application, there are reasonable grounds for believing that the person identified in the application has committed an offence under this Act. 5) No person arrested under this Act shall be denied the right of access and presence of his advocate before and during any questioning.	
32	**Powers of an authorized officer.-** (1) Subject to provisions of this Act, an authorized officer shall have the powers to – (a) have access to and inspect the operation of any specified information system; (b) use or cause to be used any specified information system to search any specified data contained in or available to such system; (c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an	**Powers of an authorised officer;-** 1) Subject to provisions of this Act, an authorised officer shall have the powers to – a) subject to grant of a warrant, have access to and inspect the operation of any specified information system; b) subject to grant of a warrant, use or cause to be used any specified information system to search any specified data contained in or available to such system; c) subject to grant of a warrant, obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system;	See Section 41 of the ETO on Immunity against disclosure of information relating to security procedure - this conflicts with it See Section 21: Powers of an Investigating Officer and Section 27: Immunity against disclosure of information relating to security procedure in PECB'14 as approved by the Cabinet Division See Necessary & Proportionate Principles on User Notification Refer to David Kaye's report, particularly IV. Enabling restrictions on encryption and anonymity, especially 45

	information system; (d) have access to or demand any information in readable and comprehensible format or plain version; (e) require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person; (f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence under this Act; and (g) require ny person who is in possession of decryption information of an information system, device or	d) subject to grant of a warrant, require any person by whom or on whose behalf, the authorised officer has reasonable cause to believe, specified information system has been used to grant access to any data within an information system within the control of such person; and e) subject to the grant of a warrant, 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; Provided, that these powers shall not empower an authorized officer to compel a suspect or an accused to provide decryption information, or to incriminate himself or provide or procure information or evidence or be a witness against himself; ***Explanation.-*** Decryption nformation 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	

	data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence. ***Explanation.-*** Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data. (2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all times shall- (a) act with proportionality; (b) take all precautions to maintain integrity and secrecy of the information system and data in respect of which a warrant for search or seizure has been issued; (c) not disrupt or interfere with the integrity or running and operation of any	information system, program or data the authorized officer at all times shall- a) Act with proportionality b) take all precautions to maintain the integrity of the information system and confidentiality of data in respect of which a warrant for search or seizure has been issued; c) not disrupt or interfere with the integrity or miming 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	

	information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued; (d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and (e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued. (3) When seizing or securing any data or information system, the authorized officer shall make all efforts to use technical measures to maintain	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.	

	its integrity and chain of custody. The authorized officer shall seize an information system, data, device or articles, in part or in whole, as a last resort only in the event where it is not possible under the circumstances to use such technical measures or where use of such technical measures by themselves shall not be sufficient to maintain the integrity and chain of custody of the data or information system being seized. (4) Where an authorized officer seizes or secures any data or information system, the authorized officer shall ensure that data or information system while in the possession or in the access of the authorized officer is not released to any other person including competitors or public at large and details including log of any action performed on the information system or data is maintained in a manner prescribed under this Act.		

33	**Dealing with seized data or information system.-** (1) If any data or information system has been seized or secured following a search or seizure under this Act, the authorized officer who undertook the search or seizure shall, at the time of the seizure,– (a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and (b) give a copy of that list to- i. the occupier of the premises; or ii. the owner of the data or information system; or iii. the person from whose possession the data or information system has been seized, in a prescribed manner in the presence of two witnesses. (2) The authorized officer, upon an application of the owner of the data or information system or an authorized agent of the owner	**Dealing with seized data.-** 1) If data has been seized or similarly secured, following a search or a seizure under Section 29 the authorised officer who undertook the search shall, at the time of the search or as soon as practicable after the search with respect to the data seized- a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and b) give a copy of that list to- i. the occupier of the premises; or ii. the person in control of the information system; or iii. a person having any legal right to the data. 2) at the time of the search and in any event not later than twenty-four hours following the seizure, the authorised officer shall- a) permit a person who had the custody or control of the information system or someone acting on their behalf to access	See Sections 23: Dealing with seized data & 24: Dealing with seized information systems PECB'14 as approved by the Cabinet Division See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See Necessary & Proportionate Principles on Integrity of Communications & Systems & Safeguards against Illegitimate Access and Right to Effective Remedy

	and on payment of prescribed costs, shall provide forensic image of the data or information system to the owner or his authorized agent within a time prescribed under this Act. (3) If he authorized officer has reasons to believe that providing forensic image of the data or information system to the owner under sub- section (2) may prejudice– (a) the investigation in connection with which the search was carried out; or (b) another ongoing investigation; or (c) any criminal proceedings that are pending or that may be brought in relation to any of those investigations, the authorized officer shall, within seven days of receipt of the application under sub-section (2), approach the Court for seeking an order not to provide copy of the seized data or information system. (4) The Court, upon receipt of an application from an authorized officer under sub-section (3), may after recording reasons in	and copy data on the information system; or b) give the person a copy of the data. 3) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that giving the access or providing the copies- a) would constitute a criminal offence; or b) would prejudice- i. the investigation in connection with which the search was carried out; ii. another on going investigation; or iii. any criminal proceedings that are pending or that may be brought in relation to any of those investigations. the Court may, after recording reasons, through written notification allow the authorised officer not to provide access or copies. 4) The Court may, on the application of: a) the occupier of the premises; or b) the person in control of the information system, or c) a person with any legal right to the data, d) on being shown sufficient cause, order that a copy be provided to such a person.	

	writing pass such order as deemed appropriate in the circumstances of the case. (5) The costs associated with the exercise of rights under this section shall be borne by the person exercising these rights.	5) The costs associated with the exercise of rights under sub-sections (2) and (4) shall be borne by the person exercising these rights. 6) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, 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.	
		34. Dealing with seized physical information systems.- 1) If an information has been physically seized or similarly secured, following a search or a seizure under section 29, the authorized officer who undertook the search must, at the time of the	

		search or in any event no later than twenty-four hours after the seizure, with respect to the physical information systems seized,- a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and b) give a copy of that list to- i. the occupier of the premises; or ii. the person in control of the information system; or iii. a person with any legal right to the data. 2) Subject to sub-section (3), on request, an authorized officer must, at the time of the search or as soon as practicable after the search,- a) permit a person who had the custody or control of the information system, or someone acting on their behalf to access and copy data on the information system; or b) give the person a copy of the data. 3) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that giving the access or providing the copies-	

		a) would constitute a criminal offence; or b) would prejudice- i. the investigation in connection with which the search was carried out; or ii. another on going investigation; or iii. any criminal proceedings that are pending or that may be brought in relation to any of those investigations. the Court may, after recording reasons, through written notification allow the authorised officer not to provide access or copies. 4) The Court may on the application of- a) the occupier of the premises; or b) the person in control of the information system, or c) a person with any legal right to the data, on being shown sufficient cause, order that a copy be provided to such a person. 5) The costs associated with the exercise of rights under sub-sections (2) and (4) shall be borne by the person exercising these rights. 6) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has	

		secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, shall be punished with imprisonment for a term which may extend to three years or with fi ne up to one million rupees or with both.	
34	**Unlawful on-line content.-** (1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to any information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.	**34. OMIT** **Please see attach petition submitted to Senate on self-regulation.**	The PTA has been given policing powers to block, remove or issue directions for removal or blocking. And any rules and standards for this can only be prescribed with the approval of the federal government. Subsection (3) states that until such time these rules or standards are framed, the Authority may exercise its powers. This section gives the government/PTA unfettered powers to block access to information or remove speech not only on the Internet but transmitted through any device. This is not only blanket censorship but also has privacy implications. It is a copy-paste of Article 19,

	(2) The Authority **"*shall,"***, with the approval of the Federal Government, prescribe rules"***for, among other matters, safeguards, transparent process and effective oversight mechanism"*** for exercise of powers under sub-section (1). (3) Until such **"rules"** are prescribed under sub- section (2), the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act. **(4) Any person aggrieved from any order passed by the Authority under sub-section (1), may file an application with the Authority for review of the order within thirty days from the date of passing of the order.**		allowing the PTA to interpret how the exclusions are to be applied. In the past, Beyghairat Bridage's video critical of the army was blocked. Shia killings, a website that documents sectarian killings, stands blocked. IMDB, a movie database was blocked because there was a review and link to a documentary on Balochistan on it. Instagram was blocked on the pretext of there being pornographic material available on it. All the alternate views found on the Mina tragedy that emerged on social media would stand blocked. No dissenting view would be available on Balochistan. As it is, several sites stand blocked on the pretext of them being 'anti-state.' Any commentary on religion or a view other one particular sect's interpretation could be blocked in the name of protecting 'the glory of Islam.' The Internet in Pakistan will become an extended version of PTV: all dissenting views would be controlled and only the state version. Sections 18, 19, 21 and 34 give PTA sole discretion over content. In the case of Sections 18 and 21, while they are non-cognizable and compoundable, the 'aggrieved' can apply directly to PTA for 'removal or destruction of, or blocking access of such information'

			and 'the Authority may on receipt of such application may take such measures as deemed appropriate fir removal or destruction of, or blocking access to, such information.' In Section 34, no one has to apply to PTA; it can act unilaterally and issue instructions as it deems fit. See Lahore High Court's interim order in the 'YouTube case,' BytesforAll vs Federation of Pakistan, and submissions made by PTA, Google and independent experts Read Islamabad High Court's order (a modified version of this initial order) in Bolo Bhi vs Federation of Pakistan, challenging the PTA and government's power to block content online See Articles 17, 18 and 19 of the ICCPR See Articles 8, 9, 10 and 18 European Convention on Human Rights See Articles 8, 9, 10 and 18 of the Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No.11 & 14) See Chapter 2 , specifically Articles 5, 8 and 10 of the American Convention on Human Rights See David Kaye's report III Encryption, anonymity and the rights to freedom of opinion and expression and

			privacy See Principles 1, 2, 5, 7, 8, 10, 11, 12, 13, 14 and 23 of the Johannesburg Principles See Manila Principles See GNI principles on Freedom of Expression and Privacy See Chapters 2, 3 and 5 of the UNESCO Report on Fostering Freedom Online: The Role of Intermediaries Refer to case: Yildirim v.Turkey And commentary by Open Society and Article 19
35	**Limitation of liability of service providers.-** (1) No service provider shall be subject to any civil or criminal liability, unless it is established that the service pro vider 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	**35. Limitation of liability of service providers.-** 1) No service provider shall he subject to any civil and criminal liability, unless it is established that the service provider had specific actual knowledge and 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	See Necessary & Proportionate Principles on User Notification See GNI principles on Freedom of Expression and Privacy

	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	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 he upon the person alleging such facts and no interim or final orders, or directions shall he 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 II)), Uniform Resource Locator (URL), Top Level Domain (TLD), Internet Protocol Addresses (11) Addresses), or other unique identifier and clearly state the statutory provision and basis of the claim. 2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in	

	Account Identification (Account ID), Uniform Resource Locator (URL), Top Level Domain (TLD), Internet Protocol Addresses (IP Addresses), or other unique identifier and clearly state the statutory provision and basis of the claim. (2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith. (3) No service provider shall be subject to any civil or criminal liability as a result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law: Provided that the service provider, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is	good faith. 3) No service provider shall he 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 by Court upon an application by an authorised officer, that demonstrates there is reasonable cause for such confidentiality and the Court shall only authorize an extension beyond fourteen days for a specified period upon an application by an authorized officer, after it is satisfied that reasonable cause for such extension exists.	

	served upon it by an authorized officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the authorized officer, the Court authorizes an extension for a further specified period upon being satisfied that reasonable cause for such extension exists. (4) No service provider shall be liable under this Act, rules made thereunder or any other law for the disclosure of any data or other information that the service provider discloses only to the extent of the provisions of this Act. (5) No service provider shall be under any obligation to proactively monitor, make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by such intermediary or service provider.	4) No service provider shall he 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 he under any obligation to proactively monitor, make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by such intermediary or service provider.	
		37. Immunity against disclosure of information relating to security procedure.- 1) Subject to sub- section (2), no person shall be	

		compelled to disclose any password, key or other secret information exclusively within his private knowledge, which enables his use of the security procedure or advanced electronic signature. 2) Subject to the right against self-incrimination under sub-section (2) of section 161 of the Code and Article 13 (2) of the Constitution, sub-section (1) shall not confer any immunity where such information is used for the commission of any offence under this Act, rules made thereunder or any other law.	
		38. Inadmissibility of seized data.- 1) Any evidence seized or similarly secured through any violation or failure to comply with any of the provisions of this Act shall have the effect of tainting the evidence seized and such evidence shall not be admissible before any Court or authority for any purpose in the relevant proceedings or any other proceedings. 2) No evidence shall be accessed, searched, seized or similarly secured unless it is relevant to the offence identified in the application and the warrant issued which shall superficially identify the particular evidence to be searched or seized is	

		issued. 3) An application to declare evidence inadmissible for the purposes of sub-section (1) or for any other reason may be moved at any time during the criminal proceedings whether during the stage of inquiry, investigation, trial, before judgment or in appeal.	
36	**Real-time collection and recording of information.-** (1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to information held by or passing through a service provider, to a designated agency as notified under the Investigation for Fair Trial Act, 2013 (I of 2013) or any other law for the time being in force having capability to collect real time information, to collect or record such information in real-time in coordination with the investigation agency	**39. Real-time collection and recording of traffic data.-** 1) If a Court is satisfied on the basis of information furnished by an authorised officer that there are reasonable grounds to believe that the content of any specifically identified electronic communication is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to traffic data held by or passing through a service provider within its jurisdiction, and where financially and technically possible for the service provider, to have that intermediary or service provider collect or record traffic data in real-time associated with only the specified communications and related to or connected with only the person under investigation transmitted by means of an information system and disclose only the specified traffic data:	Based on an application by an authorized officer, 'if a Court is satisfied that the content or any information is reasonably required for the purposed 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...having the capability to collect real time information, to collect or record such information in coordination with the investigation agency.' For a period of seven days, real-time activity will be recorded as sanctioned by court. Everything as it is being typed and transmitted would be recorded and visible. There is no mention of the capability and methods that will be used to do this – how invasive they would be. The same instruments used to record for seven days can (and most likely will) be used for continued and selective and/or broad-based surveillance.

	for provision in the prescribed manner: Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days. (2) Notwithstanding anything contained in any law to the contrary the information so collected under sub-section (1) shall be admissible in evidence. (3) The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period. (4) The Court may also require the designated agency to keep confidential the fact of the execution of any power provided for in this section and any information relating to it. (5) The application under	Provided that such real-time collection or recording shall not he 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 of time. 4) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also- a) explain why it is believed the 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) identity and explain with specificity the identified offence	See Sections 30: Real-time collection and recording of data PECB'14 as approved by the Cabinet Division See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See clause 55 in David Kaye's report under Anonymity See Necessary & Proportionate Principles on Proportionality, Competent Judicial Authority, Public Oversight, Integrity of Communications & Systems See Manila Principles V (e) about intermediaries and disclosure of identifiable information

	sub-sections (1) and (2) shall in addition to substantive grounds and reasons also- (a) explain why it is believed that the data sought will be available with the person in control of an information system; (b) identify and explain with specificity the type of information likely to be found on such information system; (c) identify and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought; (d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued; (e) specify what measures shall be taken to prepare and ensure that the real-time collection or	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 an 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. 5) Any person, including a service provider and an authorized officer, who, while providing services under the terms of lawful contract or otherwise in accordance with law, has	

	recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation; (f) explain why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and (g) why, to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.	secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, or compromises its integrity and confidentiality, 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.	
37	**Forensic laboratory.-** The Federal Government shall establish or designate a forensic laboratory, independent of the investigation agency, to provide expert opinion before the Court or for the benefit of the investigation agency in relation to electronic evidence collected for purposes of investigation and prosecution of offences under this Act.	**37. Establishment of forensic laboratory.-** 1) The Federal Government shall establish an autonomous 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.	

		2) Notwithstanding provisions of any other law, the Federal Government shall make rules, inter alia, for management and oversight of the forensic laboratory, adequate training of its staff, and provision of required resources for discharge of its functions.	
38	**Confidentiality of information.-** ***"Notwithstanding immunity granted under any other law for the time being in force,"*** person including a service provider while providing services under the terms of lawful contract or otherwise in accordance with the law, or an authorized officer who has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of lawful contract with the intent to cause or knowing that he is likely to cause harm, wrongful loss or gain to any person or compromise confidentiality of such material or data, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both.		

	(i) Provided that the burden of proof of any defense taken by an accused service provider or an authorized officer that he was acting in good faith, shall be on such a service provider or the authorized officer, as the case may be.		
CHAPTER IV: INTERNATIONAL COOPERATION			
39	**International cooperation.-** (1) The Federal Government may upon receipt of a request, ***"through the designated agency under this Act,"*** extend such cooperation to any foreign government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time	**39. 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 pursuant to the provisions of this Act. 2) The Federal Government may, at its own, forward to a foreign Government, 24 x 7 network, any foreign agency or any	Several amendments have been made to the language however the process is still missing. Suggested amendments haven't been included See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 3 & 4 See Necessary & Proportionate Principles on Safeguards for International Cooperation See Manila Principles V (e) about intermediaries and disclosure of id entifiable information

	collection of data associated with specified communications or interception of data under this Act. (2) The Federal Government may forward to a foreign government, 24 x 7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under this Act. (3) The Federal Government 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	international agency or organization any information obtained, pursuant to the provisions of this Act, 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 shall require the foreign Government, 24 x 7 network, any foreign agency or any international agency to keep the information provided confidential and use it strictly for purposes mentioned in sub-section (1) of this section. 4) The Federal Government shall be responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. Provided that the Federal Government when receiving or making a request for mutual assistance: a) Shall make and receive requests for mutual assistance through the agency established or designated under this Act	

	requests or their transmission to the authorities competent for their execution. (5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any international organization or agency if **(a) it is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interest of Pakistan;** **(b) the offence is regarded by the Federal Government as being of a political nature;** **(c) there are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons;** **(d) the request relates to an offence the**	b) Require the requesting government to make a request through the designated agency under its domestic law c) Ensure that when making or receiving a request for mutual assistance the necessary particulars are fulfilled, relating inter alia to: i. the name, address and any other relevant particulars identifying the agency making the request; ii. the specific data to which the request pertains, or its controller; iii. the purpose of the request d) The requesting agency, which has received information in reply to its own request for mutual assistance, shall not use that information for purposes other than those specified in the request for assistance e) Persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information	

	prosecution of which in the requesting State may be incompatible with the laws of Pakistan; **(e) the assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offence been the subject of investigation or prosecution under its own jurisdiction; or** **(f) the request concerns an offence which may prejudice an ongoing investigation or trial or rights of its citizens guaranteed under the Constitution of the Islamic Republic of Pakistan.** (6) Where the Federal Government decides to provide the requested cooperation, the relevant requirements and safeguards provided under this Act and rules framed thereunder shall be followed. (7) The designated agency shall maintain a register of requests received from any foreign government, 24 x 7 network, any foreign agency or any international organization or agency under this Act and action taken thereon.		

CHAPTER V: PROSECUTION AND TRIAL OF OFFENCES			
40	**Offences to be compoundable and non-cognizable.-** (1) All offences under this Act, except the offences under sections 10 and 19 **" and 19bis"**and abetment thereof, shall be non-cognizable, bailable and compoundable: Provided that offences under section 15 shall be cognizable by the investigation agency on a written complaint by the Authority. (2) Offences under sections 10 and 19 **"and 19bis"**and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency.	**40. Offences to be compoundable and non-cognizable.-** 1) All offences under this Act, except the offences section 10 of this Act, and abetment thereof, shall be non-cognizable, bailable and compoundable. 2) Offences under section 10 and abetment thereof shall he non-bailable and non-compoundable.	See Principle 22 of the Johannesburg Principles
41	**Cognizance and trial of offences.—** (1) The Federal Government, in consultation with the Chief Justice of respective High Court, shall designate presiding officers of the Courts to try offences under this Act at such places as	**41. Cognizance and trail 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	

	deemed necessary. (2) The Federal Government shall, in consultation with the Chief Justice of respective High Court, arrange for special training of the presiding officers of the Court to be conducted by an entity notified by the Federal Government for training on computer sciences, cyber forensics, electronic transactions and data protection. (3) Prosecution and trial of an offence under this Act committed by a minor shall be conducted under the Juvenile Justice System Ordinance, 2000 (XXII of 2000). (4) To the extent not inconsistent with this Act, the procedure laid down under the Code and the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), shall be followed.	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 he conducted under the Juvenile Justice System Ordinance, 2000. 4) To the extent not inconsistent with the provisions of this Act, the investigation agency and the prosecutors shall follow the procedure laid down under the Code of Criminal Procedure 1898 (V of 1898) and the Qanoon-e-Shahadat Order 1984 (President's Order No. 10 of 1984).	
42	**Order for payment of compensation.-** (1) The Court may, in addition to award of any punishment including fine under this Act, make an order for payment of compensation to the victim for any damage or loss	**42. Order for payment of compensation.-** 1) The Court may, in addition to award of any punishment including fine under this Act, make an order for payment of compensation to the victim for any damage or loss caused and the compensation so awarded	

	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.	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. Supply of statements and documents to the accused.- 1) In all cases, copies of the entire investigation file, documents related to any proceeding or investigation and all evidence, including all exculpatory facts and evidence shall be supplied free of cost to the accused not later than fourteen days before the commencement of the trial.	
		45. Description of offence to be mentioned with specificity.- The Court shall, when taking into consideration in a proceeding or mentioning any section of this Act in any document, including but not limited to any proceeding for issuance of warrant, bail, framing of charge or trial or any other proceeding with respect to or involving this Act, shall not merely consider and mention the section of the offence in question but shall also consider and	

		specify the sub-section, clause and sub clause to identify exactly which offence is being referred to.	
		46. Preliminary assessment.- 1) Upon the lodging of a report under section 155 of the Code, and again upon the filing of the interim investigation report under section 173 (1) of the Code, the Court shall, without the need for any application for such preliminary assessment to be filed, no later than the following day make a preliminary assessment under subsections (2) and (3) respectively, as to whether an offence is made out against the accused and whether there is a likelihood of conviction based upon the facts placed on record and shall as the Court may deem appropriate: a) discharge the accused; b) if an accused is not in custody and: i. the case is of further enquiry, order that no arrests be made unless the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction; or ii. if the Court is satisfied that based upon the facts placed on record an offence is made out	

		against the accused and there is a likelihood of conviction, proceed with the matter without prejudice to the right of any accused including his right to seek bail; c) if an accused is in custody and: i. the case is of further enquiry, order that the accused be released without bail subject to any future possibility of arrests if the Court is subsequently satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction; or ii. if the Court is satisfied that based upon the facts placed on record an offence is made out against the accused and there is a likelihood of conviction, proceed with the matter without prejudice to the right of any accused including his right to seek bail: Provided that any assessment under this section shall only be tentative and shall be without	

		prejudice to future determinations of the Court with respect to any further proceedings, including but not limited to bail, acquittal, framing of charge, or trial. 2) The presence of the accused shall not be necessary for any proceeding, hearing or determination under this section.	
		47. Right to pre-arrest bail.- 1) Any person whether an accused or apprehending that he may be arrested for a commission of an offence under this Act, whether or not nominated or named in any report under section 154, 155 or 173 of the Code shall have the right to seek bail and any court of competent jurisdiction shall have the power to grant him bail. 2) Notwithstanding proceedings having taken place under subsection (1), any person whether an accused or apprehending that he may be arrested for a commission of an offence under this Act, whether or not nominated or named in any report under section 154, 155 or 173 of the Code shall have the right to move an application for another preliminary proceeding under subsection (1) at	

		any stage of the case whether during the stage of inquiry, investigation, trial, before judgment or in appeal.	
		48. Pre-arrest bail when person outside Pakistan.- 1) When a person present outside the territorial limits of Pakistan comes to have knowledge of any circumstance under subsection (1) or (2) of section 42 and apprehends that he may be arrested upon his return to Pakistan for an offence under this Act, he shall have the right to seek bail or protective bail before any Court of competent jurisdiction without the need for his personal attendance and to be represented and appear by and through his pleader. 2) The Court may at its discretion make such order as to provide such a person with assurance and protection on his return and secure his attendance according to such terms as it may deem fit. 3) Should a person who has been granted bail under this section fails to return to Pakistan or abide by any of the terms thereof, the Court may cancel his bail and proclaim him an offender forthwith, ordering the investigating agency to take all	

		measures through Interpol or mutual legal assistance treaties to secure the extradition and arrest of such person.	
43	**Appointment of amicus curiae and seeking expert opinion.-** The Court may appoint amicus curiae or seek independent expert opinion on any matter connected with a case pending before it.	**49. Appointment of amicus curiae and seeking expert opinion.-** The Court may appoint amicus curiae or s eek independent expert opinion on any matter connected with a case pending before it.	
44	**Appeal.-** An appeal against the final judgment or order of a Court shall , within thirty days from the date of provision of its certified copy free of cost, lie- (a) to the High Court concerned against such judgment or order if passed by a court of sessions; or (b) to the court of sessions concerned against such judgment or order if passed by a magistrate.	**50. Appeal.-** An appeal against an order of a Court shall lie within thirty days from the date of provision of its certified copy free of cost.	
CHAPTER VI: PREVENTIVE MEASURES			
45	**Prevention of electronic crimes.-** (1) The Federal Government or the Authority, as the case may be, may issue "***directives***" to be followed by the owners of the designated	**51. 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	Refer to Manila Principles I (d) intermediaries should not be required to monitor content proactively

	information systems or service providers in the interest of preventing any offence under this Act. (2) Any owner of the information system ***"who is not a licensee of the Authority and"*** violates the guidelines issued under sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both. (3) Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996.	preventing any offence under this Act. 2) Any owner of the information system or service provider who violates the guidelines issued under sub-section (1) may be liable to be charged a fine not exceeding one million rupees, which shall be determined by the Court with the object of seeking compliance with the guidelines keeping in view of the nature of the violation and the intent of the person liable for the violation.	
46	**Computer emergency response teams.-**	**52. Computer emergency response teams.-**	

	(1) The Federal Government may constitute one or more computer emergency response teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan. (2) A computer emergency response team constituted under sub- section (1) may comprise of technical experts of known expertise officers of any intelligence or agency or any sub-set thereof. (3) A computer emergency response team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed.	1) The Federal Government may formulate one or more Computer Emergency Response Teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan. 2) A Computer Emergency Response Team constituted under sub-section (1) may comprise of technical experts from private or government sector, officers of any information agency or any sub-set thereof. 3) A Computer Emergency Response Team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed pursuant to the provisions of this Act.	
CHAPTER VII: MISCELLANEOUS			
47	**Relation of the Act with other laws.-** (1) The provisions of this	**53. Relation of the Act with other laws.-** The provisions of this Act shall	

	Act shall have effect not in derogation of the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898), the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), the Protection of Pakistan Act, 2014 (X of 2014) and the Investigation for Fair Trial Act, 2013 (I of 2013). (2) Subject to sub-section (1), the provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law on the subject for the time being in force.	have effect notwithstanding anything to the contrary contained in any other law for the time being in force.	
48	**Power to make rules.-** (1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act. (2) Without prejudice to the generality of the foregoing powers, such rules may specify- (a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors; (b) powers, functions and	**54. 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 inter alia 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	See Section 44 of the ETO

	responsibilities of the investigation agency, its officers and prosecutors; (c) standard operating procedures of the investigation agency; (d) mode and manner in which record of investigation under this Act may be maintained; (e) manner to deal with the seized data, information system, device or other articles; (f) working of joint investigation teams; (g) requirements for seeking permission of the Authority to change, alter or re-programme unique device identifier of any communication equipment by any person for research or any other legitimate purpose; (h) procedure for seeking appropriate orders of the Authority for removal, destruction or blocking access to information under this Act; (i) constitution of computer	procedures of the investigation and prosecution agency; d) mode and manner in which record of investigation under this Act may be maintained; e) working of joint investigation teams; f) qualifications and trainings of the officers, experts and staff of the forensic laboratory; g) powers, functions and responsibilities of the forensic laboratory, its officers, experts and staff; h) standard operating procedures of the forensic laboratory to interact with the investigation and prosecution agency; 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 information agencies including designated agency; l) manner of soliciting and extending international cooperation, and	

	emergency response team and the standard operating procedure to be adopted by such team; (j) appointment of designated agency having capability to collect real time information; (k) manner of coordination between the investigation agency and other law enforcement and intelligence agencies including designated agency; (l) for management and oversight of the forensic laboratory; (m) qualifications and trainings of the officers, experts and staff of the forensic laboratory; (n) powers, functions and responsibilities of the forensic laboratory, its officers, experts and staff; (o) standard operating procedures of the forensic laboratory to interact with the investigation agency; (p) manner of soliciting and	m) matters connected or ancillary thereto.	

	extending international cooperation; and (q) matters connected or ancillary thereto.		
49	**Removal of difficulties.-** If any difficulty arises in giving effect to the provisions of this Act, the Federal Government may, within two years of the commencement of this Act and by order published in the official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty.	**55. Removal of difficulties.-** If any difficulty arises in giving effect to the provisions of this Act, the Federal Government may, by order published in the official Gazette, make such guidelines not inconsistent with the guidelines of this Act as may appear to be necessary for removing the difficulty.	See Section 44 of the ETO
		56. Prior publication of rules and bylaws.- 1) All rules, bylaws and guidelines proposed to be made by the Government or the Authority, as the case may be, under this Act shall be published in the official Gazette and in at least one English and one Urdu daily with nationwide circulation, in draft form at least thirty days before the intended date of their coming into operation. 2) The Authority shall keep record of all comments received in the draft of the rules, bylaws and guidelines, and prepare a report, in consultation with the Government, addressing each comment. 3) The notification of the rules, bylaws and	

		guidelines in their final form shall be published in the official Gazette and shall be accompanied by the report of the Authority referred to in sub-section (2).	
50	**Amendment of Electronic Transactions Ordinance, 2002 (LI of 2002) and pending proceedings._** (1) Sections 36 and 37 of the Electronic Transactions Ordinance, 2002 (LI of 2002) are omitted. (2) Any action taken by or with the approval of the Authority or proceedings pending under the provisions of the Electronic Transactions Ordinance, 2002 (LI of 2002) repealed by sub-section (1), shall continue and be deemed to have been taken or initiated under this Act.	**57. 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.	
51	**Savings of powers.-** Nothing in this Act shall affect, limit or prejudice the duly authorized and lawful powers and functions of the institutions controlled by the Governments exercised and performed in good faith.	**58. 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.	