Initial analysis of Government's Proposed Amendments to PECA: March 2015

General Comments:

- Definitions have been simplified, easier to read
- Major modifications and omissions in Chapter 1, 4 and 5 subverting due process, taking out safeguards that were built in

2. DEFINITIONS

Definitions of "access to information system" and "access to data" are clearer than previous version

Additions:

(c) "Authority" means Pakistan Telecommunication Authority established under Pakistan Telecommunication (Re-organization) Act, 1996 (Act No.XVII of 1996);

(d) "authorization" includes authorization by law or the person empowered to make such authorization;

(e) "authorized officer" means an officer of the special investigation agency authorized to perform any function on behalf of the special investigation agency under this Act;

Omission

The present version defines "content data" as:

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

The following has been removed:

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

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

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

This should be reinserted

Addition:

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

Omission:

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

This definition has been completely changed – previous version provides more details on what constitutes identity information which may be necessary:

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

Addition:

(s) "intelligence" means any speech, sound, data, signal, writing, image or video;"investigating officer" means an officer of the special investigation agency designated for investigation of offences under this Act;

This has been taken from the PTA Act.

Modification:

(t) "investigating officer" means an officer of the special investigation agency designated for investigation of offences under this Act;

Previously it read:

> *"investigating officer" means an officer of the special investigation agency established under section 16;*

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

Previously it read:

> *"seize" with respect to program or data includes-*
>
> *(i) seize or similarly secure an information system or part of it or a device; or*
>
> *(ii) make and retain a copy of any program or data, including by using on-site equipment; or*
>
> *(iii) render inaccessible, or remove, data in the accessed information system; or*
>
> *(iv) obtain output of data from an information system;*

(x) "service provider" includes-

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

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

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

(iv) any person who provides premises from where or facilities through which the public in general may access information systems and the internet such as cyber cafes;

(iv) has been modified, previously it read as follows:

> *(iv) any person who, as a core business or a substantial part of his business provides premises from where and facilities through which the public in general may as customers access information systems and the internet such as cyber cafes; or*
>
> *(v) any person who as a core business or a substantial part of his business, provides a network for distribution of electronic communication;*

(iv) in its current form is problematic because it seems to suggest any place that either houses information systems or provides access to the Internet such as offices, restaurants, places such as T2F, Kuch Khaas and The Nest, are service providers. Should revert to previous version where, only if the provision of facilities is part of 'a core business or substantial part of the business' should this definition apply.

Comment:

bb) "unauthorized access" means access to an information system or data without authorisation or in violation of the terms and conditions of the authorization;

As noted previously, this is prone to abuse and needs to be defined (as does authorization) so users have a fair idea. Additionally, what would constitute authorization, consent and in what form would it have to be given. Can this be applied to, for example the terms and conditions of websites or applications, which no one actually reads?

See: http://www.washingtonpost.com/politics/as-cyberthreats-mount-hackers-conviction-fuels-critics-claims-of-government-overreach/2013/04/29/d9430e3c-a1f4-11e2-9c03-6952ff305f35_story.html

cc) "unauthorised interception" shall mean in relation to an information system or data, any interception without authorization;

Where is authorized interception mentioned and what are the limitations and procedural requirements for it?

Addition:

(3) Other expressions used in the Act or rules framed under it but not defined herein, unless their context provides otherwise, shall have meanings assigned to the expressions in the Pakistan Penal Code 1860, Code of Criminal Procedure 1898 and 'Qanoon-e-Shahadat Order 1984, as the case may be.

This has been added.

CHAPTER 1: OFFENCES & PUNISHMENTS

Authorization is defined as: *includes authorization by law or the person empowered to make such authorization;*

And unauthorized access as: *access to an information system or data without authorisation or in violation of the terms and conditions of the authorization;*

With respect to Sections 3 & 4 which are as follows:

> ***3. Unauthorized access to information system or data**.- (1) Whoever with malicious intent gains unauthorized access to any information system or 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.*
>
> ***4. Unauthorized copying or transmission of data.-** Whoever with malicious intent and without authorization copies or otherwise transmits or causes to be transmitted, any data whether by gaining access to such data or otherwise, 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.*

It is not clear what would constitute authorization by law or otherwise. Moreover, in what form would the authorization be required i.e. in writing? Example, what if someone verbally authorized another to access a system or copy a file, but later withdraws that authorization or simply denies that the authorization was ever given. What recourse would there be for someone who is then charged for unauthorized access?

Section 8

In the modified version, the cyber terrorism clause reads as follows:

> *8. **Cyber terrorism**. –Whoever commits or threatens to commit any of the offences under sections 5 and 7 where-*
>
> *(a) the use or threat is designed to coerce, intimidate, overawe or create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or*
>
> *(b) the use or threat is made for the purpose or motive of advancing a religious, ethnic or sectarian cause;*
>
> *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.*

The definition of Cyber Terror has been picked up from the Anti-Terrorism Act, which in itself is a bit ambiguous. The law should clearly require establishment of intent. Sub-clause (b) for

example, speaks of promoting religious/ethnic cause, which is not terrorism per se, unless pursued to create a sense of fear or insecurity in society.

This entire clause needs to be revisited – it uses vague terms and is loosely worded. The language needs to be tightened; it should read 'use **and** threat' not 'use **or** threat.' A 'perceived threat' should not be criminalized and the phrase should be removed. In its current form, it is unclear what type of crime the clause pertains to even though we understand that it relates to Sections 5 & 7, which are as follows:

> ***5. Unauthorized access to critical infrastructure information system or data.-*** *Whoever with malicious intent gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment upto three years or with fine which may extend to one million rupees or with both.*
>
> ***7. Criminal Interference with critical infrastructure information system or data.-*** *Whoever with malicious intent and without authorization interferes with or damages, or causes to be inferred with or damaged, any critical information system or any part thereof, or critical infrastructure data or any part thereof, shall be punished with imprisonment which may extend to seven years or with fine which may extend to five million rupees or with both.*

This is because the following from the previous draft has been omitted:

> *(i) interfering with, disrupting or damaging a public utility service or a communications system used by the public at large;*
>
> *(ii) severe interference with, seriously disrupting or seriously damaging a designated payment system which interconnects with multiple financial institutions;*
>
> *(iii) severe interference with, seriously disrupting or seriously damaging a mass transportation or mass traffic system;*
>
> *(iv) severe interference with, seriously disrupting or seriously damaging a critical infrastructure that is used to serve a public function for the public at large;*
>
> *(v) severe interference with, seriously disrupting or seriously damaging critical infrastructure in use by the armed forces, civil armed forces, security forces or law enforcement agencies;*
>
> *(vi) causes injury through the acts mentioned in clauses (i), (iii), (iv) and (v); or*
>
> *(vii) enabling any of the things mentioned in sub-clauses (i) to (vi) to be done,*
>
> *shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.*
>
> *(2) Whoever commits any offence under sub-section (1) of this section by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.*
>
> *(3) The intention referred to in sub-section (1) need not relate to—*
> *(a) any particular information system;*
>
> *(b) any particular program or data; or*

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

(4) In this section—
(a) a reference to doing an act includes a reference to causing an act to be done;

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

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

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

(i) by or through an automated mechanism and self-executing, adaptive or autonomous device, program or information system;
(ii) against Government controlled information systems or public information systems in exercise of a public function: or

(iii) against any information system.

The above should be reinserted to add clarity and limit the scope of the crime and its application. Without this clause is extremely vague and open to abuse.

The other thing to consider is whether access and damage to critical infrastructure should be separate offences (currently as separate offences they carry lower punishments) or, since they relate to this clause, should they be merged in this section and removed as separate offences. And, if retained in their current form, would there be a risk of a person being charged either twice, or under cyber terrorism instead because it carrier a higher sentence?

Section 9

In the modified version, forgery is as follows:

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

(2) Whoever commits 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 five years or with fine which may extend to five million rupees or with both.

This was defined as follows in the previous version:

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

(a) without authority;

(b) in excess of authority; or

(c) through an unauthorised act,

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

(2) Whoever commits an offence under subsection (1), dishonestly or with similar intent, -
(a) for wrongful gain;

(b) for wrongful loss; or

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

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

(3) Whoever commits an offence under subsection (1), fraudulently, dishonestly or with similar intent, -
(a) to influence a public servant in the exercise of a public duty or function; or

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

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

How are damage or injury construed? Shouldn't the definition of what constitutes forgery be clearer? Some explanation/illustration (in fact with most crimes) would be useful as there is in Section 17.

Section 10

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

Again, how are damage or injury construed?

In the previous version, electronic fraud was defined as follows:

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

(a) without authority;
(b) in excess of authority; or
(c) through an unauthorised act, causes loss, in whole or in part, of any data or program, property, valuable security or consideration to another person or any information system by-

(a) any illegal access to information system or illegal access to program or data;
(b) any input, alteration, modification, deletion, suppression or generation of any program or

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

with fraudulent or dishonest intent to cause-

(i) wrongful gain;
(ii) wrongful loss; or
(iii) any economic benefit for oneself or for another person,

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

The descriptions of the crime are necessary for context and should remain for Sections 9 & 10. What requires clarity is how the impact/loss will be assessed.

The "or" between inducing any person to enter into a relationship and intent to deceive should be taken out so that both inducement and intent form components of the offence.

Section 11

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

Does believing (and the highlighted clause) need to be there at all? Just limit it to 'intending it primarily to be used.'

Section 12

*12. **Identity crime**.- (1) Whoever obtains, sells, possesses or transmits another person's identity information, without lawful justification 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.*

(2) Any person whose identity information is obtained, sold, possessed or retains may apply to the Court competent to try offence under sub-section (1) for passing of such others as the Court may deem fit in the circumstances for securing, destruction or preventing transmission of any such data.

What is 'lawful justification' and where is this defined? This should be defined better so there is no ambiguity in terms of what would constitute legal and illegal use. For example, would my ID card, used or displayed without my permission, be an identity crime? Often television channels broadcast details, not necessarily with consent, authorization, or 'lawful justification.'

How does this apply to information held by telcos, ISPs, companies etc in terms of how data is held and shared. We know third parties collect and buy user information. Would that be criminalized too? Ideally such clarity should be drawn through Data Protection & Privacy legislation, both of which we do not have. Which is why in the absence of them, it becomes all the more necessary to create those distinctions in this law.

Moreover, what comprises identity information? The previous draft contained a detailed definition, which is as follows:

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

This has been removed in the current version and now reads:

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

The language ought to be tightened and illustrations provided to give the court guidance into what would be "unlawful justification" i.e. Which forms of transmission of identity are being criminalised and which are not. The current language and over broad and leaves completely to the discretion of court to determine the scope of this offence and the possible defences against it.

Section 13 & 14

> ***13. Unauthroized issuance of SIM cards etc.-*** *Whoever sells or otherwise provide subscriber identity module (SIM) card, re-usable identification module (R-IUM) or other portable memory chip designed to be used in cellular mobile or wireless phone for transmitting and receiving of intelligence without obtaining and verification of the subscriber's antecedents in the mode and manner 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 both.*
>
> ***14. Tempering etc. of communication equipment.-*** *Whoever changes, alters, tampers with or re-programs unique device identifier or international mobile station equipment identity (IMEI) number of any stolen cellular or wireless handset and unlawfully or without authorization starts using or marketing it for transmitting and receiving intelligence through such mobile or wireless handsets shall be punished with imprisonment which may extend to three years or with fine which may extend to 1 million rupees or both.*

These sections have been added into the current version. Wouldn't it be more appropriate to add these to either the PTA Act or ETO? In the previous version Chapter 5: Section 47 excluded telco related offences from this bill. See below:

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

Section 15:

*15. **Unauthorized interception**.- Whoever intentionally commits unauthorized interception by technical means of-*
(a) any transmission that is not intended to be and is not open to the public, 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:

Some example here would be useful to understand what is and is not considered 'open to public.' There is need to define "transmission" to exclude harmless interception such as use of wi-fi signals.

Also, how does this apply to intelligence agencies and the government is also unclear. In the previous version, the paragraphs below followed the stipulated punishment:

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

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

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

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

(a) for wrongful gain; or
(b) for wrongful loss; or
(c) for any economic benefit for oneself or for another person,

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

There is mention of a warrant for authorized or legal interception, which has been removed in the current version. Must also be noted that Section 48 referenced above has also been removed in its entirety from the modified version. However the omission of Section 48 may not be too bad since it exempted the application of anything in this Act to the 'activities, powers or functions of intelligence agencies. The section was as follows:

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

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

Still, Section 15 requires more clarity and some checks and balances should apply, even to intelligence agencies.

Section 16

*16. **Offence against dignity of natural person**- (1) Whoever, with malicious intent, knowingly and publicly exhibits, displays, transmits any electronic communication that ~~harms the reputation of a natural person,~~ threatens any sexual acts against a natural person; superimposes a photograph of the face of a natural person over any sexually explicit images; ~~distorts the face of a natural person;~~ or includes a photograph or a video of a natural person in sexually explicit conduct, without the express or implied consent of the person in question, intending that such electronic communication cause that person injury ~~or threatens injury to his or her reputation,~~ his or her existing state of privacy or puts him or her in fear for him or her safety shall be punished with imprisonment for a term which may extend to one year or with fine which may extend to one million rupees or with both.*

(2) Whoever commits an offence under sub-section (1) with respect to a minor, shall be punished with imprisonment for a term which may extend to three 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, may apply to the court for passing of such orders for removal, destruction or blocking access to such material referred in sub-section (1) and the Court on receipt of such application may pass such orders as deemed proper in the circumstances.

It is good that this has been changed to 'a natural person.' However the highlighted clauses (that have been struck out) need to be removed. This section should pertain only to sexual acts or sexually explicit images and content.

Express or implied consent is problematic. Firstly, how would either of these be established and, if established, what other laws could be used against the person issuing the consent?

Shouldn't a provision be created where someone else can appear on behalf of the complainant even if he/she is not a minor? Given our prevalent socio-cultural norms and environment, particularly in the case of a woman, she would most likely hesitate to approach the police or courts herself.

The 'removal, destruction and blocking access to such material' has to be evaluated. Firstly, this should also apply to court records too – the image or video in question. There should be a clear policy of keeping such information private and ensure it is not transmitted/disseminated from police/court. Some protections have to be built in for that too, in terms of how such data is handled, retained and ultimately destroyed. The second aspect would be its transmission otherwise. The way to deal with this is by criminalizing the act of recording, transmitting such material under law so that is acts as a deterrent.

As in the case of the recent rape incident where a gang-rape was recorded and circulated, and transmitted through Bluetooth and phone applications, it becomes virtually impossible to control, block or destroy such data, especially when it is not in a centralized location. Then it will also boil down to a question of what is possible and within reasonable and legal parameters.

Also the following parts have been removed from the modified version, which guaranteed certain protections, and should be reinserted for clarity and so that this section is not misused in any way:

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

This is especially important if the phrases that have been struck out i.e harm to reputation and distortion of face remain.

Section 17:

17. Malicious code.- *Whoever wilfully 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 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 both:*

Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of any code for any lawful purpose:

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

Just like an exception and explanation is provided in this section, similarly, for the sake of clarity, the same should be added to other sections (some of those mentioned if not all).

Section 18

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

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

commits the offence of cyber stalking.

(2) Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment for a term which may extend to two years or with fine which may extend to one

million rupees, or with both:

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

(3) Any person may apply to the court for issuance of a restraining order against an accused of cyber stalking and the court upon receipt of such application may pass such order as deemed appropriate in the circumstances of the case.

This is over broad.

Cyber stalking, as an offence, has been added in the modified version. Clauses a, b and c are extremely vague and should be removed. Clause e will also need to be better defined. Also, cyber-stalking currently carries a greater punishment than Section 16, which deals with sexually explicit content in relation to a person.

Newspapers for example use images of politicians, celebrities or other public figures, not necessarily with consent or knowledge. Same goes for memes that circulate on social media. Exceptions that were built into Section 16 in the previous draft should be added here too. See below:

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

Section 19

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

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

This has been added in as an offence into the modified draft. The Akram Sheikh version also contained spamming as an offence. Firstly, 'harmful, fraudulent, misleading' are vague terms. 'Unsolicited' and 'without the express permission' are problematic; if someone sends another an email, a forwarded email for instance, would that be considered spam? And aren't spam filters in inboxes, or settings in mobile phones to block certain numbers enough to deal with this problem, rather than trying to address this through law. Application and parameters within which this can or will be applied are unclear. Should be removed.

Presently "unsolicited intelligence" would cover advertisements as well. This offence should also be narrowly defined in such manner that it only covers such spamming activities that are targeted to cause a breakdown or impairment of an information system.

Section 20

> ***20. Spoofing.-*** *(1) Whoever dishonestly, establishes a website or sends any intelligence 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 may extend to five hundred thousand rupees or with both.*

Like Section 19, this has been added into the modified version and were offences in the Akram Sheikh bill – which was a copy paste job of the Indian IT Act (the defunct version, prior to amendments). There are different kinds of spoofing i.e. email spoofing, IP spoofing. It is a type of electronic fraud, identity crime and malicious code – depending on the type or manner of spoofing. Therefore, since it is a variant, it should be dealt with under already existing sections instead of creating a separate offence for it.

Section 21

> *21.* ***Legal recognition of offences committed in relation to information systems****.- (1) Notwithstanding anything contained in any other law, an offence under this Act or any other law shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to, or through the use of, an information system.*
> *(2) References to "property" in any law creating an offence in relation to or concerning property, shall include information systems and data.*
> *(3) References in any law creating an offence to an act shall include actions taken or caused by use of an information system.*
> *(4) References to an act by a person in this Act or any law establishing an offence shall include acts done or to be done by or through automated mechanisms and self-executing, adaptive or autonomous devices, programs or information systems.*

How this applies and what are the implications needs to be looked into.

Section 22

> ***22. 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.*

This has been added.

CHAPTER 2: ESTABLISHMENT OF INVESTIGATION & PROSECUTION AGENCY AND PROCEDURAL POWERS FOR INVESTIGATION

Section 23

*23. **Establishment of investigation agencies and prosecution**.-(1) The Federal Government shall designate the Federal Investigation Agency or any other law enforcement agency as the special investigation agency for the purposes of investigation and prosecution of offences under this Act.*
(2) Unless otherwise provided for under this Act the special investigation agency, the special investigating officer, prosecution and the court shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act.
(3) The Government shall organize specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the special investigation agency.

At a time, there should be only one special investigation agency, preferably designated through this Act and not at a later time by the federal government. At the moment, the language of this section leaves it open for the government to designate FIA or any other law-enforcement agency as the special investigation agency (does that mean an existing law-enforcement agency)? Perhaps the addition of the word 'existing' before law-enforcement agency should be made.

In the event that a new agency needs to be constituted, it is a given that it can only be constituted through an Act of parliament and not an executive order by setting up a body? How can this be mandated under this Act?

The first paragraph should be amended to read as follows:

"*The federal government shall designate the Federal Investigation Agency or designate any other law-enforcement agencies as the special investigation agency for the purpose of investigation and prosecution of offences* ***provided that the power, functions or provisions shall only be exercised in accordance with the procedure and provisions specified for each of those procedures and provisions under this Act."***

This is to ensure that the law-enforcement agency/special investigation agency is bound by the procedures of this Act, so excesses can be curbed. However, a lot of the procedural protections that existed have been removed (highlighted and discussed later).

What has been removed from this section, which was present in the previous version is as follows:

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

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

(3) above from the previous draft should replace the modified version because this mandates an officer to hold a qualification in digital forensics etc whereas the modified version simply suggests that the government, as a matter of awareness and capacity building, will organize courses. There is a huge difference between the two. Moreover, even though the language of the previous draft should be employed, somewhere it should be clarified exactly what kind of a qualification is required.

There should be one designated specialized agency. Otherwise all intelligence agencies will end up becoming designated agencies, resulting in overlap of authority, turf-wars and lack of accountability.

Section 24

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

Provided that the Federal Government or the Provincial Government may, as the case may be, constitute joint investigation team comprising of the officers of special investigation agency and any other law enforcement agency including Police for investigation of events involving commission of offences under this Act and any other law for the time being in force.

(2) No person other than a prosecutor designated as such by the special investigating agency shall prosecute any offence under this Act.

The highlighted portion above has been added into the modified draft and should be removed. It negates the first paragraph. You don't want multiple people/agencies handling data and devices etc., because excesses and violations would then go unchecked, it would be hard to hold any one person or agency responsible, as they'll deflect.

Other qualifications that were present in the previous version have been omitted. These are as follows:

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

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

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

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

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

These are important as they lay down parameters within which an investigating officer must carry out duties and should be reinserted.

Section 25

> *25. **Expedited Preservation of data**.- (1) If an investigating officer is satisfied that-*
>
> *(a) data stored in any information system or by means of an information system, is reasonably required for the purposes of a criminal investigation; and*
>
> *(b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the investigating officer may, by written notice given to a person in control of the information system, require the person to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice.*
>
> *(2) The period provided in sub-section (1) for preservation of data may be extended by the Magistrate if so deemed necessary upon receipt of an application from the investigating officer in this behalf.*

Why should it be left up to the satisfaction and determination of an investigating officer instead of requiring the officer to go through court? The duration in the modified version has been increased to ninety days from seven days and should be reversed. Moreover, the following clause, has been removed, which should be reinserted:

> *(3) The person in control of the information system shall only be responsible to preserve the data specified-*
> *(a) for the period of the preservation and maintenance of integrity notice or for any extension thereof permitted by the Court;*
> *(b) to the extent that such preservation and maintenance of integrity will not be administratively or financially burdensome; and*
> *(c) where it is technically and practically reasonable to preserve and maintain the integrity of such data.*

This protects a person or service providers from being subjected to unrealistic and cumbersome directives, which they may not be able to comply with.

Section 26

> ***26. Retention of traffic data.---(1)** A service provider shall, within its existing or required technical capability, retain its traffic data for a minimum period of ninety days or such period as the Authority may notify from time to time and provide that data to the special investigating agency or the investigating officer whenever so required.*
>
> *(2) The service providers shall retain the traffic data under sub section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transaction Ordinance, 2002 (LI of 2002).*
>
> *(3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to six months or with fine which may extend to or with both.*

This section has been modified. The previous version read as follows:

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

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

In its current form, this section empowers the Authority (which as per the amended definitions stands for PTA) to extend the retention period and require service providers to provide that data to the special investigation agency or officer, without going through court. Why is PTA being brought into this process (is it because under it's Act it is empowered to issue directives to ISPs and they don't want these powers to be distributed to any other agency)? Here too, like in Section 25, an officer should have to go to court to extend the duration of the retention period.

The addition of (3) not only mandates service providers to retain data but also criminalizes, it seems, a person/service provider who does not retain traffic data. This should be taken out.

Section 27

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

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

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

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

Major changes have been made to this section. Prior to amendments it read as follows:

***Warrant for search and seizure**.-(1) Upon an application on oath by an investigating officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, program, data, device or storage medium of a specified kind that-*
(a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or

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

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

the specified information system, program or generally present or available at the specified place:

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

The previous version required for the application to be 'on oath' (under oath?); this has been removed. Then, the search and seizure was limited to '**only**' a 'specified place' and a 'specified kind' of medium, not just miscellaneous 'other articles' as the language of the modified version now reads. Only has been replaced with '**any**' making the application of this section too broad. Then, previously the section also required the court to record reasons before issuing a warrant. This too has been omitted.

Furthermore, a list of qualifications with regards to the application and what it must cite has been completely removed. This was as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

The above omitted section required investigation officers to provide detailed reasoning. It required the court to depute a Magistrate to accompany the officer – one who had no connection to the special investigation agency in any way – and restrained the court from issuing a warrant for the search and seizure of **'any'** premises, information system etc unless after investigation on the basis of specified contents of the application fell short of yielding results and thereafter required broader access.

A penalty was also prescribed for anyone who acted misused powers under this, maintaining a check and balance. Furthermore, citizens were protected against self-incrimination.

These are extremely important procedural safeguards and must be reinserted.

Section 28

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

Again, the requirement for the application to be 'on oath' (under oath?) has been removed. The other modification allows the court to order a person in control of the information system or data to 'provide data or access' to the investigating officer. Previously, the clause required the person in control of the information only to 'disclose sufficient traffic data about a specified communication.' Not hand over data or access to such data. That too, the communication a person was required to disclose was for the explicit purpose of 'identify[ing]' the following:

(a) the service providers; and

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

Other qualifications with regards to the application and what it should contain have been completely removed, which are as follows:

(3) The application under sub-section (1) shall in addition to substantive grounds and reasons also:
(a) explain why it is believed the traffic data sought will be available with the person in control

of the information system;

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

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

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

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

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

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

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

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

Again, the protections provided earlier, against self-incrimination and misuse of power, have been removed and need to be put back in.

Section 29

*29. **Powers of an investigating officer**.-(1) Subject to provisions of this Act, an investigating officer shall have the powers to -*

While there is an insinuation that the investigation officer would seek a warrant/permission before exercising some of the powers vested in him, the prerequisite for seeking such warrant should be clearly stated.
This previously read as follows:

*Subject to obtaining a search warrant under section 19 an investigation officer shall be entitled to **only** the information system, program and data **specified** in the warrant to-*

Section 19 i.e. referred to above pertained to warrant for search and seizure, much of which has been changed in the modified version (refer to analysis of Section 27 above). The clauses listed below were subject to the investigation officer first having attained a warrant, requirement for which, under the modified version, does not exist. This should be reversed.

(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 information system;
(c) obtain and copy any data, use equipment to make copies and obtain an intelligible output from an information system;
(d) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such information

system into readable and comprehensible format or plain version;
(e) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any information system has been used to grant access to any data within any information system within the control of such person;
(f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the investigating officer may require for investigation of an offence under this Act; and
(g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence:

The following clause, which followed the above clauses, has been omitted from the modified version.

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

This protected against self-incrimination and also restrains an investigating officer from gaining access decryption information. This must be reinserted.

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 investigating officer shall-

(a) at all times act with proportionality;
(b) take all precautions to maintain integrity of the information system and data subject of the search or seizure in respect of which a warrant has been issued;
(c) not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued;
(d) avoid disruption to the continued legitimate business operations and the premises subject of the search or seizure; and
(e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued.

(3) When seizing or similarly securing any information system or data, the investigating officer shall make all efforts to use technical measures while maintaining its integrity and chain of custody and shall only seize any information system, data, device or articles, in whole or in part, as a last resort, for sufficient reasons that do not make it possible under the circumstances to use such technical measures or where use of such technical measures by themselves would not be sufficient to maintain the integrity and chain of custody of the data being seized.

The clause that followed the above clauses, and has been omitted from the modified version was as follows:

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

seizure before the Court.

This needs to be reinserted. Also an entire section that followed powers of investigation officers i.e. cordons on investigation, has been completely removed. It read as follows:

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

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

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

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

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

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

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

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

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

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

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

Section 30

*30. **Dealing with seized data.-**(1) The Federal Government may prescribe rules for dealing with the information system, data or other articles seized under this Act.*

This has been left to the discretion of the federal government and must not be allowed. In the previous version, this section read as follows:

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

(b) give a copy of that list to-

(i) the occupier of the premises; or
(ii) the person in control of the information system; or
(iii) a person having any legal right to the data.

(2) Subject to sub-section (3), at the time of the search and in any event not later than twenty-four hours following the seizure, the investigating officer shall-
(a) permit a person who had the custody or control of the information system or someone acting on their behalf to access and copy data on the information system; or
(b) give the person a copy of the data.

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

(b) would prejudice-

(i) the investigation in connection with which the search was carried out;
(ii) another ongoing investigation; or
(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

(4) The Court may, on the application of:
(a) the occupier of the premises; or

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

(c) a person with any legal right to the data,
on being shown sufficient cause, order that a copy be provided to such a person.

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

The above procedure is necessary to retain. However, the highlighted clause should be revisited. Why should an investigation make this determination? Especially where the provision of copies is concerned. The reasonable grounds should at the very least be determined by a court, and an investigation officer should be required to submit reasons for denial of information etc.

Also, while the modified version vaguely mentions dealing with information systems under the same section, previously a separate section dealt with seizure of information system, which is as follows:

Dealing with seized physical information systems*.-(1) If an information has been physically seized or similarly secured, following a search or a seizure under section 18, the*

investigating officer who undertook the search must, at the time of the search or in any event no later than twenty-four hours after the seizure, with respect to the physical information systems seized,-
(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to-

(i) the occupier of the premises; or
(ii) the person in control of the information system; or
(iii) a person with any legal right to the data.

(2) Subject to sub-section (3), on request, an investigating officer or another authorized person must, at the time of the search or as soon as practicable after the search,-
(a) permit a person who had the custody or control of the information system, or someone acting on their behalf to access and copy data on the information system; or
(b) give the person a copy of the data.

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

(b) would prejudice-

(i) the investigation in connection with which the search was carried out; or
(ii) another ongoing investigation; or
(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

(4) The Court may on the application of-
(a) the occupier of the premises; or
(b) the person in control of the information system, or
(c) a person with any legal right to the data,
on being shown sufficient cause, order that a copy be provided to such a person.

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

Clause 3 (highlighted) as with the previous section is problematic. Same concerns and suggestions apply as mentioned above.

The following section has been completely removed:

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

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

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

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

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

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

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

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

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

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

(6) Simultaneous to the arrest of the person identified in the application the investigating officer shall inform such person that-
(a) he has the right to remain silent;

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

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

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

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

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

(9) Any person arrested under this Act shall have the right to-
(a) not make any statement;

(b) not answer any questions;

(c) to remain silent; and

(d) have his advocate present.

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

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

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

'I have explained to (…name…) that:
(a) he has a right to remain silent
(b) anything he says can and shall be used against him in the court of law;
(c) that he has the right to communicate and consult with an advocate as well as have his advocate present at all times during an when being questioned or making any statement or confession
(d) if he cannot afford an advocate he may elect to have the specialized investigation agency immediately appoint an advocate for him and subsequently also have the Court appoint a different advocate for him, if he so elects, when he appears before the Court next morning.
(e) he is not under any compulsion whether direct or indirect to make any statement or any confession
(f) if he does make a statement or confession can and shall be used as evidence against him which would open him to being convicted of an offence.

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

Explanation. It shall not be necessary that the Magistrate or specially designated investigation officer receiving and recording a confession or statement should be a Magistrate having jurisdiction in the case or an investigation officer involved in the investigation of the case.
(12) Only evidence of statements or questioning conducted and documented through video

and audio recording shall be admitted before any Court whether as evidence or otherwise.

This needs to be reinserted.

Section 31

In the modified version, the following has been added:

31. Power to issue directions for removal or blocking of access of any intelligence through any information system: *(1) The Authority or any officer authorized by it in this behalf may direct any service provider, to remove any intelligence or block access to such intelligence , 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, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, commission of or incitement to an offence.*

(2) The Federal Government may prescribe rules for adoption of standards and procedure by the Authority to monitor and block access and entertain complaints under this section. Until such procedures and standards are prescribed, the Authority shall monitor and block intelligence in accordance with the directions issued by the Federal Government.

This needs to be taken out. It has been inserted for the simple reason to amass blocking powers to exert control over content on the Internet. It mixes language of Article 19 and the definition of 'intelligence' in the PTA Act (which the government seems to think is a stand in for content).

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

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

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

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

(3) No intermediary or service provider shall be subject to any civil or criminal liability as a

result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law.

Provided that the intermediary or service provider present and established in terms equivalent to the requirements of the Companies Ordinance 1984 within the territorial jurisdiction of Pakistan, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served upon them by an investigating officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the investigating officer, the Court authorizes an extension for a further specified period of time, upon being satisfied that reasonable cause for such extension exists.

(4) No intermediary or service provider shall be liable under this Act, rules made thereunder or any other law for the disclosure of any data or other information that the service provider discloses only to the extent of and under sub-section (3) and sections 25, 27, 28 and 29.

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

Confidentiality and non-disclosure clause is problematic. Why shouldn't this disclosure be made?

The sections that followed the above one have been omitted and are as follows:

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

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

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

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

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

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

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

cognizance of the matter and proceed in accordance with the Code.

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

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

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

These should be reinserted.

Sections 33, 34, 35, 36

The sections below have been added to the modified version of the bill:

33. Information in cognizable cases.- *(1) Information relating to the commission of a cognizable offence under this Act if given orally to an officer of the special investigation agency authorized in this behalf, shall be reduced to writing by him or under his direction and then read over to the informant and every such information, whether given in writing or reduced to writing as aforesaid, shall be signed by the person giving it, and the substance thereof shall be entered in a book to be kept by such officer in such form as the Federal Government may prescribe in this behalf.*

34. Information in non-cognizable cases: *(1) When information is given to an officer of special investigation agency authorized in this behalf of the commission of a non cognizable offence, he shall enter in a book to be kept as aforesaid the substance of such information and refer the information to the Court.*

35. Investigation into cognizable cases: *Any authorized officer of the special investigation agency may, without the order of the Court, investigate any cognizable case.*

36. ***Investigation into non-cognizable cases.-*** *No officer of the special investigation agency shall investigate a non cognizable case without the order of the Court.*
(2) Any officer of the special investigation agency receiving such order may exercise, the, same powers in respect of the investigation (except the power to arrest without warrant) as an officer incharge of a police-station may exercise in a cognizable case.

There is no need to draw a distinction between the procedures of cognizable and non-cognizable cases. The deleted provisions (cited before this section) should be reinserted and the procedures in them should be followed. Under no circumstances should investigations without warrants (and other procedural requirements) be carried out.

Section 37

37. ***Real-time collection and recording of data****.-(1) Notwithstanding anything contained in Investigation for Fair Trials Act 2013 (Act No.I of 2013) or any other law for the time in force, if a Court is satisfied on the basis of information furnished by an investigating officer that there are reasonable grounds to believe that the content of any intelligence or data is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to intelligence or data held by or passing through a service provider, to the service provider to collect or record such data in real-time in coordination with the special investigation agency:*

The highlighted portions are modifications that have been made to this clause. Previously the same clause read as follows:

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

The modified version references the Fair Trial Act. How does impact the application of this section? Then, as per the modified version, an investigation officer is not required to furnish information under oath whereas previously he was required to.

'Specifically identified electronic information' has been replaced by 'intelligence or data,' which is too broad. Similarly, 'traffic data or content data' has also been replaced with 'intelligence and data.'

The above-mentioned data, previously, was limited to a service provider within the court's jurisdiction whereas in the modified version the term 'jurisdiction' has been removed. Further, the modified version allows the collection and recording of data by a service provider 'in coordination with the specialized investigation agency' which absolutely must not be permitted. If at all this needs to be done, the court, service provider and agency should remain independent of each other – be it the collection or provision of information.

The following clauses which preceded the list that follows, have been omitted from the modified version:

> *(a) have that service provider collect or record traffic data in real-time; and*
>
> *(b) and where administratively and financially not burdensome and technically possible, collect or record content data in real-time, conducted only through, in coordination with and facilitated by the intelligence agency or intelligence service referred to in section 48 of this Act and specially notified in respect of and for the purposes of this section by the Federal Government through notification in the Official Gazette, associated with only the specified communications and related to or connected with only the person under investigation transmitted by means of an information system and provide only the specified traffic data and where applicable content data, to the investigating officer:*

Some minor modifications have been made to the clauses below:

> *Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event not for more than seven days.*
>
> *(2) The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period of time.*
>
> *(3) The Court may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.*
>
> *(4) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also-*
>
> *(a) explain why it is believed the data sought will be available with the person in control of the information system;*

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

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

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

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

(f) why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and

(g) why to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.

Previously, clause 4a and 4b were restricted to 'traffic' data however now they simply include 'data.'

The following clauses have been removed:

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

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

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

A separate section that dealt with retention of traffic data has been omitted. This was as follows:

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

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

CHAPTER 2: INTERNATIONAL COOPERATION

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

(2) The Federal Government may, without prior request, forward to such foreign Government, 24 x 7 network, any foreign agency or any international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other Government or agency in initiating or carrying out investigations or proceedings concerning any offence.

(3) The Federal Government may require the foreign Government, 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 investigating agency shall be responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

(5) The Federal Government may refuse to accede to any request made by such foreign Government, 24 x 7 network, any foreign agency or any international agency if the request concerns an offence which is likely to prejudice its sovereignty, security, public order or other national interests.

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

The major issue with this section is that it is broad and does not specify how our governments and agencies will interact with foreign governments and agencies, how the requests will be made, how data will exchanged etc. Especially troubling is the clause "the federal government may, without prior request, forward to such foreign government."

The concern here is specifically how data is currently changing hands between the Pakistan government and companies. Recently, Facebook turned over IPs to the FIA. Right now the language of the law is too broad. The aim of amending this clause is to limit anybody that holds data - be it a government authority or private company - whether local or international, to turn over data without a warrant and due process that the investigating agency is required to follow under this law. This is especially necessary since we so now have data protection and privacy laws, therefore such protections need to be built into this Act.

The following should be added at the end of clause 1: *"provided that the power, functions or provisions shall only be exercised in accordance with the procedure and provisions specified for each of those procedures and provisions under this Act."*

The power, functions and procedures should be consistent with the highlighted changes that have been recommended, which means reinserting a lot of the deleted provisions to ensure due process and that safeguards for citizens remain in place.

CHAPTER 4: PROSECUTION AND TRAIL OF OFFENCES

Section 40

*40. **Cognizance and trial of offences**.— (1) The Federal Government, in consultation with the Chief Justice of respective High Court, shall designate Magistrates and Session Judges at such districts or places as deemed necessary who shall be competent to try the offences under this Act.*
(2) Notwithstanding the provisions of provincial public service commission laws, the designated judges under sub-section (1) shall have successfully completed training conducted by the Federal Judicial Academy with respect to all aspects of this Act including cyber forensics, electronic transactions and data protection.

(3) All offences under this Act, except offence under section 8 and abetment thereof, shall be cognizable and tried by the Magistrate designated under sub-section (1).

(3) Offence under section 8 and abetment thereof shall be tried by the Sessions Judge designated under sub-section (1).

(4) In all matters with respect to which no procedure has been provided in this Act, the provisions of the Code and Qanun-e-Shahadat . 1984 (X of 1984) shall apply.

Previously, it was the Court of Sessions empowered to try cases see definition from previous draft:

(a) "the Court" means the Court of Sessions competent to try offences under this Act;

There was no mention of the federal government consulting with Chief Justices and designating magistrates and session judges. The government should not be involved to this extent.

Secondly, a period for the training should be specified i.e. 6 months and it should be mandated that only after completing the training should they be able to preside over cases. See relevant section from the previous draft (this has been omitted in the modified version).

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

The modified version draws a distinction between what a magistrate can try and what a sessions judge can try, particularly for Section 8. Why shouldn't all the offences be tried by a sessions judge – in fact that should be the criteria by default.

The addition also references Qanun-e-Shahadat, which wasn't there previously.

There appear to be some typo in Section 40(3). It appears from Section 39 that all offences under this law are non-cognizable and bailable, except cyber terrorism which is cognizable (even though Section 40(3) says the opposite thing). This scheme will be abused as the investigation agency will start registering cases under Section 8 (cyber terror) because that will be cognizable, even if later the offence of terror isn't established. It is thus essential to (i)

make all offences non-cognizable, even if terror etc are non-bailable and non-compoundable, and (ii) as an extension clearly state that getting court permission/warrant is a pre-requisite to initiating investigation etc. The same principle should apply even where information is being sought through international cooperation.

Section 41

*41. **Order for payment of compensation**.- (1) The Court may, on awarding punishment of imprisonment or fine or both for commission of any offence, make an order for payment of any compensation to the victim for any damage caused by commission of the offence and the compensation so awarded shall be recoverable as arrears of land revenue:*

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

(2) Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (Act V of 1898), it shall be lawful for the Court to award any compensation authorized by this Act even if such compensation exceeds its powers under the Code.

Clause 2 has been modified, previously it read as follows:

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

The following sections have been completely removed from the modified version:

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

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

*38. **Supply of statements and documents to the accused**.- (1) In all cases, copies of the entire investigation file, documents related to any proceeding or investigation and all evidence, including all exculpatory facts and evidence shall be supplied free of cost to the accused not later than fourteen days before the commencement of the trial:*
Provided that the Court may direct that the cost of any storage devices required for supplying such copies may be paid by the accused in case the Court is satisfied that, for reasons to be recorded, the accused has access to such funds that would enable the accused to make such payment.

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

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

(2) The High Courts shall maintain a list of such amicus curiae having the relevant

qualifications and experience.

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

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

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

(b) technical experts; or

(c) forensic experts

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

*41. **Preliminary assessment**.- (1) Upon the lodging of a report under section 155 of the Code, and again upon the filing of the interim investigation report under section 173 (1) of the Code, the Court shall, without the need for any application for such preliminary assessment to be filed, no later than the following day make a preliminary assessment under subsections (2) and (3) respectively, as to whether an offence is made out against the accused and whether there is a likelihood of conviction based upon the facts placed on record and shall as the Court may deem appropriate:*
(a) discharge the accused;

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

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

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

(c) if an accused is in custody and:

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

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

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

(2) The presence of the accused shall not be necessary for any proceeding, hearing or

determination under this section.

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

(2) Notwithstanding proceedings having taken place under subsection (1), any person whether an accused or apprehending that he may be arrested for a commission of an offence under this Act, whether or not nominated or named in any report under section 154, 155 or 173 of the Code shall have the right to move an application for another preliminary proceeding under subsection (1) at any stage of the case whether during the stage of inquiry, investigation, trial, before judgment or in appeal.

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

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

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

*44. **Manner of recording evidence**.- For the purpose of recording evidence in all proceedings under this Act before a Court, the evidence of the witnesses shall be recorded in the following manner-*
Entire Inquiry, Trial and all proceeding before the Court shall be video and audio recorded and copy of the same shall be made available to the accused directly or to his pleader as well as the prosecutor and the complainant directly or to his pleader by the close of the day of each proceeding:

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

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

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

form.

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

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

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

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

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

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

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

48. ***Savings of Intelligence Services powers****.- (1) Offences, powers and procedures provided under this Act are not related to and have no application upon the activities, powers or functions of intelligence agencies or services and are without prejudice to the operation of or powers-*
(a) under section 54 of the Pakistan Telecommunication (Re-organization) Act, 1996;
(b) under the Army Act, 1952;
(c) under the Air Force Act, 1953;
(d) under the Navy Ordinance, 1961;
(e) under the purview of the Intelligence Bureau;
(f) by the intelligence agency or intelligence service notified by the Federal Government under section 30 of this Act; and
(g) when exercised lawfully by any other intelligence agency or service that by itself does not investigate or prosecute an offence.

49. ***Act to override other laws****.-The provisions of this Act shall have effect notwithstanding*

anything to the contrary contained in any other law and shall survive any amendment of any other law unless specifically amended or repealed.

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

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

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

CHAPTER 5: MISCELLANEOUS

Section 43:

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

Previously, the relevant section read as follows:

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

Section 44

44. Power to make rules.- *The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act.*

In the previous version, the relevant section was as follows:

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

Section 45

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

This has been added in.