Initial Analysis of PECB as Passed by the National Assembly: April 2016

The word "intentionally" has been replaced with "with dishonest intention" in Sections 3, 4, 5, 6, 7, 8, 9 and 17. In Section 23 "dishonestly" has been replaced with "with dishonest intention."

It was earlier recommended "malicious intent" be added to all clauses. What needs to be discussed further is what "dishonest intention" constitutes and its place in existing jurisprudence, whether is adequate as mens rea or should be replaced with "malicious intent" as was earlier suggested.

With regards to Sections 3,4, 6 & 7, their potential to be misapplied to whistleblowers and journalists remains a huge concern. In an environment where even though freedom of information is recognized by the Constitution and legislation to enable access to it exists, the culture is still to deny information and exclusionary clauses are cited more often than not, to ensure it is not shared. Leaked information is how the whistle is blown on a lot of overreach by governments, their organizations and others. While information must surely not be used to blackmail intimidate or scandalize people, however certain information only finds it way into the public domain when it is leaked and someone blows the whistle on it. The right balance must be struck which cannot be done by changing the language of this alone but ensuring that enabling legislation with protections for data, whistleblowing etc are in place to draw from.

Section 9: Glorification of an offence and hate speech - has been amended. "commission or threat" has been removed and sub sections (a) and (b have been clubbed together so that now it reads in continuity. Language of the rest of the clause has also been slightly altered.

However the major contention in this clause, i.e. "the intent to glorify an offence and the person *accused or convicted* of a crime relating to terrorism" remains. What of those accused and held under the Anti-Terrorism Act: the I-11 protestors or those in Okara. Individuals and groups campaigning for the release of those wrongly booked of crimes, advocating for the quashing of cases etc could be charged on the pretext of glorifying the alleged offence or person, even though it is an appeal for justice and due process.

Section 10: Cyber terrorism – the word "religious" in (b) has been replaced with "inter-faith" and "discord" with "hatred." The word "overawe" has been removed. This section carries a jail term of fourteen years and a fine of up to fifty million rupees. The language is incredibly vague and this is a cognizable offence How this will be determined is not clear. While this applies in relation to Sections 6,7, 8 and 9, chances are, people will either be booked under both sections or the higher penalty will be invoked.

This is a cognizable offence which non-bailable and non-compoundable.

Section 18: Offences against dignity of natural person – "which he knows to be false" has been added and "likely to" before "harm to reputation" has been omitted. This section criminalizes the act of exhibiting, displaying or transmitting information a person "knows to be false" that "harms or intimidate the reputation or privacy of a natural person." This carries a jail term of up to three years and a fine up to one million rupees.

While this doesn't apply to anything aired on television, it applies to everything uploaded and shared online. Political expression and satire is not exempted. Some examples how this can be misapplied:

The person who uploaded Rehman Malik's video of boarding a flight late would be jailed for it. In fact he did lose his job and was charged under the Maintenance of Public Order. PTI activist Qazi Jalal was charged under Section 36 & 37 of the ETO for a tweet in which he alleged a judge's son-in-law was deriving benefits due to his in-laws' position. He included a wedding card in his tweet to corroborate the person in question was actually the son-in-law. In Turkey, a man is facing a two-year jail term for sharing a meme comparing Erdogan and Gollum – character from the Lord Of The Rings Trilogy. Would the same happen to person who created/shared the Nawaz Sharif & Shrek meme? And any other form of political expression, satire or citizen journalism will be construed as harm to reputation. Either people will start to self-censor – as is now rampant on channels and do a great degree in print – or people will have FIRs lodged against them and face jail terms. We already have defamation laws and there is no need to criminalize defamation.

The following addition has been made to Sections 19 and 21: "and the Authority may also direct any of its licensees to secure such information including traffic data." What the practices to secure such information are not defined. Securing traffic data under this Act does not require a warrant. In the Philippines, the real-time collection of traffic data clause in their cybercrime law was struck down by the Supreme Court in 2014 Technology activists were successful in making their case before court that even traffic data was identifiable data and therefore its collection infringed privacy and opened doors to mass surveillance.

In the absence of data protection and privacy legislation, this cannot be left up to the discretion of an executive authority.

Already Sections 18, 19 and 21 allow the 'aggrieved' to apply directly to the PTA for 'removal or destruction of, or blocking access of such information' 'the Authority on receipt of such application, may pass such orders as deemed appropriate including an order for removal, destruction of, or blocking access to, such information.'

Section 19: Offences against modesty of a natural person and minor –
"or video" has been added to sub section (a)
"or any sexually explicit image or video of a natural person" added to (c)

new sub section (d) has been added which reads "cultivates, entices or induces a natural person to engage in a sexually explicit act" with the following addition after it:

"through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail."

The offence if committed with respect to a minor, carries a jail term and fine, whereas previously it was imprisonment or fine.

A proviso and new sub section [see (3) has been added]

The terms "makes available, distributes or transmits" in sub section (3) can be slightly problematic with regards to drawing attention to such issues. When the Kasur incident took place it was only when the videos were released to the public, that it came to the fore. What would be the repercussions on individuals or media outlets who do so? Recently footage of a woman being harassed at a political rally was aired and circulated on social media. The ethics of this method - releasing footage to the public and the appropriate manner in which this should be done – can be debated. There are two aspects. Releasing such footage is used as a means of drawing attention to the issue which otherwise is swept under the carpet, and it also acts as proof. However on the other it impacts the privacy of the person involved is something that needs to be discussed. This requires careful consideration in terms of how it is to be dealt with versus setting huge criminal penalties that may extend to the above scenarios.

Moreover, this too is a cognizable offence which non-bailable and non-compoundable.

Section 21: Cyber Stalking – the language has been slightly altered. Sub sections (a)-(c) have been replaced with new clauses.

The addition of "make a video" has been made to (d)

(d) can have wide connotations. What about pictures taken without permission if they are covering crowds at public events? Or those pictures zeroing in on public/known figures attending rallies/congregations by banned organizations, in an attempt to call them out or hold them accountable for it? This carries a jail term of up to three years.

Again, it is not court but the PTA to whom the 'aggrieved" party can apply just like Sections 18 and 19. And the following addition has been made to this section too: "and the Authority may also direct any of its licensees to secure such information including traffic data."

22: Spamming – The definition of spamming is incredibly vague. This section criminalizes the transmission of "has been criminalized. It is unclear as to how one should acquire permission. This will disrupt the very nature of public messaging relied on not only by businesses and political parties, but rights

defenders and entrepreneurs. There is no need to include such a provision in a criminal law, or criminalize the act. There are other ways of dealing with this, particularly through the existing telecommunications regulatory regime or, through tools available in mobile phones and email inboxes. People should not be jailed for what is an irritant.

28. Expedited preservation and acquisition of data – An 'authorized officer' may write to a person in control of an information system and require him/her to provide data or order that specified data be preserved up to 90 days. It is after this is done that the authorized officer must bring this to the court's attention within 24 hours. So post-PECB, we will be receiving written orders from not even the agency but an officer, to hand over data. 24 hours is long enough a period to misuse the powers given.

29: Retention of data – a service provider (i.e. ISP) is required to retain data (of its customers) up to a year and provide it to the investigation agency or authorized officer as and when notified by the Authority to do so. Our entire digital footprint – what we accessed, who we communicated with and the specific contents – would be on offer. Also, retention of data is quite costly and this will be an added expense for service providers.

31: Warrant for content data – this section pertains to the 'disclosure of content data.' It speaks nothing of data other than content data. In this bill, data is defined as 'traffic data and content data.' Moreover other forms of 'data' are covered under other definitions. Information for instance is defined as: 'text, message, data, voice, sound, database, video, signals, software, computer programs, any form of intelligence as defined under the PTA (Reorganization Act 1996 and codes including object code and source code.'

So while a warrant would be required for disclosure of 'content data,' there is no procedure nor oversight prescribed for the acquisition, disclosure, retention, preservation or handling of traffic data – which is also identifiable data (i.e. can reveal a person's location, identity and more. Nor does this exist for information – the definition for which contains nearly all forms of data. Moreover Section 31 deals with a person in control of the information system or data, and not service providers or those storing data on behalf of others. Therefore the token warrant for content data hardly serves as a safeguard for the above-listed sections, which give sweeping powers over - and intrusive access - to everyone's communication and data. And there is no data protection or privacy legislation in Pakistan.

34: Unlawful online content – Three minor changes have been made to this section. The title has been changed from "power to manage online content" to unlawful online content." The reference to service providers has been removed, leaving it even more open ended for PTA to issue takedown orders to whomever they wish.

The following has been added to subsection (2) The Authority may, *with the approval of the Federal Government*, prescribe rules for adoption of standards

and procedure for exercise of powers under sub-section (1).

The PTA has been given policing powers to block, remove or issue directions for removal or blocking. And any rules and standards for this can only be prescribed with the approval of the federal government. Subsection (3) states that until such time these rules or standards are framed, the Authority may exercise its powers.

This section gives the government/PTA unfettered powers to block access to information or remove speech not only on the Internet but transmitted through any device. This is not only blanket censorship but also has privacy implications. It is a copy-paste of Article 19, allowing the PTA to interpret how the exclusions are to be applied.

In the past, Beyghairat Bridage's video critical of the army was blocked. Shia killings, a website that documents sectarian killings, stands blocked. IMDB, a movie database was blocked because there was a review and link to a documentary on Balochistan on it. Instagram was blocked on the pretext of there being pornographic material available on it.

All the alternate views found on the Mina tragedy that emerged on social media would stand blocked. No dissenting view would be available on Balochistan. As it is, several sites stand blocked on the pretext of them being 'anti-state.' Any commentary on religion or a view other one particular sect's interpretation could be blocked in the name of protecting 'the glory of Islam.' The Internet in Pakistan will become an extended version of PTV: all dissenting views would be controlled and only the state version.

Sections 18, 19, 21 and 34 give PTA sole discretion over content. In the case of Sections 18 and 21, while they are non-cognizable and compoundable, the 'aggrieved' can apply directly to PTA for 'removal or destruction of, or blocking access of such information' and 'the Authority may on receipt of such application may take such measures as deemed appropriate fir removal or destruction of, or blocking access to, such information.' In Section 34, no one has to apply to PTA; it can act unilaterally and issue instructions as it deems fit.

36. Real-time collection and recording of information – Based on an application by an authorized officer, 'if a Court is satisfied that the content or any information is reasonably required for the purposed of a specific criminal investigation, the court may order with respect to information held by or passing through a service provider, to a designated agency...having the capability to collect real time information, to collect or record such information in coordination with the investigation agency.' For a period of seven days, real-time activity will be recorded as sanctioned by court. Everything as it is being typed and transmitted would be recorded and visible. There is no mention of the capability and methods that will be used to do this – how invasive they would be. The same instruments used to record for seven days can (and most likely will) be used for continued and selective and/or broad-based surveillance.