Proposed Amendments to the Prevention of Electronic Crimes Bill 2015

To Omit:

Section 15: Unauthorized issuance of SIM cards – This makes operators criminally liable whereas this is an already regulated sector and the policy directives and existing laws apply.

Section 18: Offences against the dignity of a natural person – Section 19 criminalizes the misuse of photographs and information in sexually explicit conduct. Given that, and the fact that a defamation law already exists, there is no need for this section since it deals with reputational damage. Moreover an exemption has been created only for the broadcast media and not others. Previously Section 18 & 19 were compounded together and a proviso existed that protected speech made in good faith or as an act of political expression etc. Most problematic is that the redress mechanism stipulated flows through not court, but the PTA, allowing for misuse not only by complainants but also the Authority, since it has been left up to its discretion what should be removed or blocked based on a complaint.

Section 22: Spamming –The transmission of 'unsolicited intelligence' without the 'express permission of the recipient' has been criminalized as per the language of this clause. It is unclear as to how one should acquire express permission. Definition of spamming also not provided. Spamming can be curtailed through filters in email inboxes for example, number-blocking options in mobile phones. This should be dealt with through policy guidelines and a regulatory framework, not as a criminal offence.

Section 34: Power to Manage intelligence and issue directions for removal of blocking of access of any intelligence through any information system – this clause gives the government/PTA unfettered powers to block access or remove speech not only on the Internet but transmitted through any device, through its own determination. Not only does this infringe fundamental rights of citizens but also curbs media freedom. The government would be able to acquire powers to order media houses' web platforms to remove any material they deem inappropriate. Example: criticism of the government or a view contrary to theirs could be removed on the grounds – according to them – that it is 'anti-state' or against 'national interest.' Such excessive powers are unconstitutional. As it is, the government and PTA's blocking powers stand challenged in court and this matter is therefore sub judice. They should wait for a resolution of the case instead of trying to hastily create a provision in law to try and legitimize their blocking powers, influence court proceedings and pre-empt a judgment.

To Amend:

Z aa) Definition of **service provider** needs to be amended. iii) is extremely vague. As per the definition in clause iv) service providers – traditionally ISPs and telecom operators - has been expanded to now include any place that offers access to the Internet, to the public, i.e., restaurants, malls, hotels, airports, stations and the additional burden of retaining traffic data has been placed on them – and they can be punished for not doing so. This is unrealistic and increases the cost of business.

Section 9: Glorification of an offence and hate speech – the 'preparation' of intelligence has also been criminalized even if it is not disseminated. This section carries an imprisonment term of five years. Instead of 'Whoever prepares **or** disseminates,' this should at the very least be changed to 'Whoever prepares **and** disseminates' so there is a clear cause and effect, and they are read in conjunction with one another. Next, (a) reads 'glorify an offence or person **accused** or convicted.' The word accused should be removed, since the crime has not been established. Only convicted should remain.

Section 10: Cyber Terrorism – the clause reads 'whoever **threatens** to commit any offence.' This section carries an imprisonment term of fourteen years. While the commission of an offence should be punishable, anything can be construed as a threat. This section also requires a proviso for ethical hacking/white-hat hackers, hobbyists who conduct activities to identify security breaches in systems. It should also protect teenagers from getting implicated as cyber terrorists and jailed for fourteen years, for something they may have done out of boredom – which needs to be reprimanded and dealt with differently.

Sections 18: Natural Dignity of a Person, 19: Offenses against the modesty of a natural person and minor and 21: Cyber Stalking, allow complaints to be made directly to the PTA. The determination of the offence and required action has been left to its discretion. None of these clauses – which can easily be misused by the complainants or the Authority, require going to court.

Clause [2] from sections **18, 19 and 21** should be omitted. Determination of the offense, grievance and

relief should be subjected to a court process rather than be decided arbitrarily by an executive authority. The court can, in turn, order the relevant authority to take appropriate action once the offence has been established, but executive authorities must not play judge, jury and executioner.

Section 21: Cyber Stalking – sub-sections (a) to (c) contain vague terms such as 'obscene, vulgar, contemptuous, indecent and immoral. These sub-sections should be omitted. The language in (d) needs to be tightened as this could be broadly applied to public events that are covered by the media or political parties, where consent is not explicitly sought before taking pictures are taken or distributed. Similarly, pictures of public figures are carried in articles to supplement them, or memes are created. Harm could be misused and misapplied to settle scores. Therefore a clear balance needs to be struck in this clause so it does not criminalize commonplace activity – for those ethical guidelines can be developed. A proviso should be inserted that excludes the use of pictures for legitimate use, political expression, satire etc.

Section 38: Offences to be compoundable and non-cognizable – 19 i.e. Offences against the modesty of a person should be removed. Only 10 i.e. Cyber terrorism should remain as a non-bailable offence.

Section 42: **Appeal –** An appeal should not be limited to only the final judgment of court and the provision for an appeal to be made before a High Court should exist

To Add:

dd) Definition of **unauthorized access** needs to be elaborated on, especially when read together with **Sections 3 & 4** on unauthorized access to system or data and copying or transmission. In what form would authorization be required is unclear. If someone verbally authorized another to use their laptop, which is a common practice among peers and colleagues, and then to malign the individual the authorizer decided to maintain authorization was never given and there exists no proof of it, that would become punishable? Sections **3 & 4** should also contain a proviso/exception for whistle-blower protection. Otherwise an act such as acquiring and disseminating copies of this bill for instance would be criminalized. The state could use this to control information and hold records that should be made public, but would remain classified and illegal to acquire.

Section 11: Electronic Forgery and **Section 12: Electronic Fraud** should contain explanations or illustrations due to the technical nature of these offenses, to assist the court in establishing the crime. There should also be an assessment process to determine the degree of damage so punishment is awarded proportionately. Some mention should also be made of recourse available to a person to retrieve information/data and be compensated for loss.

Section 20: Malicious Code – A proviso/exception needs to be created for this clause. What may be deemed as 'malicious codes' or 'viruses' are taught and written as part of academic disciplines. That is how software is developed to combat them. An exception for this should be clearly stipulated or it would create a sense of fear among academics of being potentially charged for a crime, and create hesitation to apply what is learnt in this discipline for legitimate purposes. Moreover, most USBs carry viruses – oftentimes without the knowledge of the owner. Scenarios in which unwittingly a USB transmits a virus should be accounted for. The manner in which this offence would be determined should be specified in clearer terms.

Section 27: No warrant, search, seizure or other power not provided for in the Act - The officer should have to go to court and require a warrant for search, seizure and arrest

Section 32: Powers of an authorized officer – Exercise of powers should be subject clear checks and balances to curtail misuse since this section contains intrusive powers. Moreover, (g) requires decryption information to be divulged. This will have adverse implications especially on the industry, in terms of data security, and no foreign company would be willing to sign an MoU with a local company if security can be infringed in this manner. This should be removed.

Section 33: Dealing with seized data – Currently this has been left to the discretion of the federal government, while it should be clearly stipulated under this Act (as it was in the stakeholder version).

Section 37: International Cooperation – In the absence of data protection and privacy legislation, it is essential a process be formulated and stipulated in this law that creates a framework within which data of Pakistani citizens is to be acquired and exchanged with other foreign companies and governments.