Why do we need a cybercrime law?

- Internet and technology have been recognized as great enablers in creating new opportunities for business, paving way for a thriving culture of entrepreneurship and innovation (also social); breaking down literacy barriers; facilitating the democratization of systems; connecting people and societies, and providing platforms for dialogue and exchange of views between citizens around the world. Knowledge, information as well as the ability to communicate lies at one's fingertips now like never before.

- With the arrival of smartphones, even a mobile phone is now a computing device. According to the Pakistan Telecommunication Authority's (PTA) July 2015 report, the total teledensity in Pakistan stands at 63.6%. There are 116,431,523 annual cellular subscribers. 3G/4G Subscribers stand at: 14,614,411. The figures for broadband subscribers by technology are 18,001,252 (Mobile BB: 14,614,411).

- While much good has come from the easy access and spread of technology, this space is not free of dangers or criminal activity. Where there are positive, legal uses of technology, there are negative and illegal uses as well. Compromised email or social media accounts are a common occurrence that plague the average Internet and technology user, leading in turn to other misuses and crimes such as data and identity theft. Such activities impact the average user, businesses and the government.

- Due to the nature of this medium, often existing laws are found wanting to cover the wide spectrum of crimes unique to this medium, which necessitates a law of a very specific nature – both in terms of the offences it creates and the procedures to deal with them. There is no disagreement over the fact that a cybercrime law is the need of the hour. However, given that there is still relatively low computer and technology literacy in the country, a law that deals with crimes needs to be carefully crafted. While it should serve the rightful purpose of curtailing criminal activity, it should not place the fear of technology among a people still embracing and learning to use this medium. Neither should it treat every user as a potential criminal.

What's wrong with the proposed bill

- The fundamental flaw with the government's proposed Prevention of Electronic Crimes Bill is that it tries to kill too many birds with one stone – and disproportionately at that. There is no distinction between telecom offences, cybercrimes and social ills – they have all been packed into one law and criminalized.

- The proposed bill does not distinguish between innocent people and criminals, neither does it exempt or cater for accidental breaches. In turn, it prescribes heavy penalties in the form of jail terms and fines, and even criminalizes acts such as spamming, which can be dealt with in other ways rather than through imprisonment.

- Much is left to the discretion of authorized officers, authorities and agencies, and the federal government. Overbroad powers have been given to regulatory and investigation bodies without any checks and balances or accountability mechanisms. Too much is left to the rule-making powers of the government. Judicial oversight, with the exception of requiring warrants for search and seizure, remains absent in the proposed law.

- Loosely worded sections leave too much room for interpretation and misinterpretation, widening the window for misuse and likelihood of the provisions of this bill being used for score-settling rather than addressing criminality.

- Blanket censorship, curtailment of political speech, dissenting views and debate and dialogue will be sanctioned should Sections 9, 18 and Section 34 come to pass.

- A tremendous amount of liability is placed on businesses and service providers – including criminal penalties which directly conflict with the intermediary liability protection extended to them under the same law – which will create a stifling environment for them to operate it, while discouraging entrepreneurs and small and medium enterprises from setting up and operating.

- Some of the most problematic sections of the bill are as follows:

1. Definition of ***unauthorized access*** and Sections 3-4 & 6-7 do not create an exception for whistleblowers, white-hat hackers and hobbyists who, under this law would land up in jail for their activities, which are not categorized as criminal otherwise.
2. Definition of ***offence*** makes children as young as 13 culpable under this bill
3. ***Section 9: Glorification of an offence and hate speech*** criminalizes even the 'preparation' of information even if it is not disseminated. To advocate for a person wrongly accused or convicted of a crime would not just be illegal but punishable by five years in prison or with a fine up to ten million rupees or both. Critiques of judgments – which are commonplace - could also be criminalized, as would be any voices highlighting miscarriage of justice as they could be misconstrued as 'glorifying' an accused or convicted person.
4. ***Section 15: Unauthorised issuance of SIM cards etc*** is a telecom offence that should be dealt with under the PTA Act. Telecom already is a heavily regulated sector. Moreover, imposing criminal penalties conflicts with intermediary liability protection extended through Section 35.
5. ***Sections 18: Natural Dignity of a Person*** deals with reputational damage already covered under the Defamation Act. Political expression, satire is not exempted. This will

impact social media users and online platforms of media outlets. Moreover, rather than authority resting with a judicial body i.e. court, to determine the very subjective nature of this offence, powers instead have been delegated to the PTA to play judge, jury and executioner.

6. ***Section 21: Cyber Stalking,*** crimalizes the transmission of 'obscene, vulgar, indecent, immoral' material which could be interpreted as anything and misapplied. Moreover, there is no exemption for pictures taken without permission if they are covering crowds at public events, which impacts media coverage. And this section carries a jail term.
7. ***Section 22: Spamming,*** the transmission of 'unsolicited information' without the 'express permission of the recipient' has been criminalized. It is unclear as to how one should acquire express permission. This will disrupt the very nature of public messaging relied on not only by businesses but political parties, educational institutes and other organizations. There is no need to include this in this law, or criminalize the act.
8. ***Section 27: No warrant, search, seizure or other power not provided for in the Act:*** too much if left to the discretion of government authorities, no judicial oversight, especially data-related sections.
9. ***Section 29: Retention of data*** runs contrary to the right to privacy. In the absence of privacy and data protection legislation, this puts at risk the data of citizens to misuse by authorities and others who may gain access to it. Also, this already exists in the Electronic Transactions Ordinance (ETO), so there is no need to add it here too.
10. **Section 32: Powers of an authorized officer** are very broad and not subjected to judicial oversight. They are particularly invasive of the privacy and the potential for misuse is extremely high. Sub-section (g) which requires the disclosure of encryption keys (passwords etc), forces an individual - and by default those connected to him her – to divulge and provide access to private data beyond what may be necessary or within the scope of the investigation. It also poses a risk to companies who are required to sign confidentiality agreements or MoUs for business.
11. **Section 33: Dealing with seized data**: Currently this has been left to the discretion of the federal government and its rule-making powers, while the procedure should clearly be stipulated under this bill (as it was in the stakeholder version). Data is sensitive information and how it is seized, handled and preserved needs clear and stringent guidelines.
12. ***Section 34:*** 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. It is a copy-paste of Article 19, allowing the PTA to interpret how the exclusions are to be applied.
13. **Section 37: International Cooperation**. This section gives the federal government unbridled powers to share information with international governments/agencies without any oversight. Again, in the absence of privacy and data protection legislation, it becomes all the more essential a process be formulated and stipulated under this law that creates a framework within which data of Pakistani citizens is to be acquired and exchanged with other foreign companies and governments.
14. ***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.

What are we proposing?

- The use of technology to commit a crime does not make it a cybercrime by definition. The guiding principle for the construction of this law should be that only those offences that occur in electronic form in the cyber world and are not already covered under Pakistan Penal Code (PPC) or in any other law/form should be a part of this legislation. Practically any offence under the PPC can be facilitated through electronic means. This does not mean that all offences of the PPC should be covered under the PECB nor does the use of electronic means make it a cybercrime.

- Speech-related offences and those that pertain to the telecom sector should be omitted from this bill; only computer/medium specific crimes should remain.

- The age distinguishing a minor and an adult should be 18.

- 'Malicious intent' should be added to all sections on offences to establish mens rea.

- Warrants should be required for not only search and seizure, but for all offences. An officer should have to provide reasoning before court as to why access to a person's data, device or to the accused himself/herself is necessary.

- Procedures should be defined under this law rather than left up to the rule-making powers of the government. Moreover, the rule-making powers of the government should also be subjected to public scrutiny – all proposed rules should go through the public eye before coming into effect.

- Penalties should exist for service providers and investigation officers who step beyond the scope of duty and misuse information they may gain access to – especially in the absence of privacy and data protection legislation.

- Cooperation with foreign governments and entities – and on what terms – should be subjected to a well-defined procedure stipulated under this law.

- Privacy, due process and oversight should, under no circumstances, be compromised.

Cybercrime law: Facts

A timeline of cybercrime laws in Pakistan is as follows:

- Pervez Musharraf promulgated the Prevention of Electronic Crimes Ordinance in 2007, which expired in 2009. When during the PPP tenure efforts were made to write the ordinance into law, the move was opposed by industry and civil society groups, and members of opposition. Then Prime Minister Yousuf Raza Gilani withdrew it from the floor of the assembly.
- Following the withdrawal of this bill, industry associations, together with members of opposition and later Ministry of Information Technology and Telecom, the Federal Investigation Agency and security agencies, drafted a Prevention of Electronic Crimes Bill, which was submitted to the Cabinet Division in 2014.
- In 2014, two other bills were floated. One, a private members bill tabled by Senator Karim Khuwaja. And a second commissioned by the Prime Minister's office to Akram Sheikh Associates.
- What made it to parliament was a modified version of what came to be known as the industry stakeholder bill, approved by the Cabinet Division in February 2015. This was soon replaced by an entirely new government bill as of April 2015 on the pretext of aligning it with the National Action Plan.
- During this time period, Sections 36 and 37 of the Electronic Transactions Ordinance have been used to prosecute people for certain electronic crimes.

- According to research, out of 196 countries in the world, approximately 75 countries have some form of cyber laws. Most countries have multiple legislations - some distinguish between e-commerce legislation and cyber crime legislation, while others address both in one piece of legislation.

- It is generally standard practice to refer to international best practices, covenants and conventions when drafting a law. The Budapest Convention is referred to when drafting cybercrime laws, which serves as a guideline on offences and procedures. Offences listed in the Budapest Convention typically relate to illegal access, illegal interference with systems, identity theft, fraud, child pornography. Fifty countries are signatory to this convention and 47 have ratified it. Pakistan is not one of them.

- The other important international document to consult is the International Covenant on Civil and Political Rights (ICCPR), which has 74 signatories and has been ratified by 168 countries - including Pakistan. This outlines a basic human rights framework, outlines fundamental freedoms nations must uphold, and processes that must be applied when devising laws. This takes precedence.