Note on the Bills

Offences:

Both bills contain offences, some of which are similar in nature – illegal or unauthorized entry and interference with an information system; electronic fraud and forgery; cyber extremism or terrorism; violation of privacy/offence against dignity. Other comparable sections include expedited preservation of data and real-time collection and recording of data.

The government's proposed bill creates a new set of offence. A few examples are as follows: unauthorized copying and transmission of data; glorification of an offence and hate speech; unauthorized use of identity information; unauthorized issuance of SIMs; spamming; spoofing; power to manage online information etc.

Powers and Procedures:

In the government's proposed Prevention of Electronic Crimes Bill, warrants are required for search and seizure, disclosure of content data, real-time collection and recording of information. Warrants for arrest are not specified and sections 10 and 19 are cognizable offences, allowing officers to arrest without warrants.

In Senator Karim Khuwaja's bill, exercise of powers especially with respect to arrest, search, seizure and collection of data – are subject to warrants and court oversight. With the exception of expedited preservation of data, which can be ordered by an officer of the special investigation agency, but the data must be preserved by the person in control of the information system.

Senator Karim Khuwaja's bill also lists detailed procedures that must be followed in terms of obtaining warrants, down to what the application by an authorized officer must contain and what should be deemed acceptable by Court, while the government does not do so and simply stipulates the requirement for a warrant but not the particulars that must be specified.

Courts, Agencies and Authorities

Senator Karim Khuwaja's bill seeks to create Special courts for the trial of offences, whereas the government's bill specifies a court of competent jurisdiction; however it creates the provision to appoint presiding officers in consultation with the chief justices of the High Court, to try offences under the proposed law. Senator Karim Khuwaja's bill seeks to establish a new investigation agency whereas the government's bill leaves room for either a new agency to be established or, an existing agency to be designated as the investigation agency.

The government bill, while it does not name the investigation agency, includes the Pakistan Telecommunication Authority by name. The bill allows requests with respect to Sections 18, 19 and 21 to be made directly to it and empowers it to take cognizance and act unilaterally. Under Section 34, it empowers the authority to determine the nature of the offence and doesn't even require a complainant to act and implement directives. For these sections, neither the complainant nor the Authority are required to go through court. This is left to executive discretion.

A view from around the world

Two international conventions and covenants become relevant in the drafting of this particular law. The International Covenant on Civil Political Rights (ICCPR), and the Council of Europe's Budapest Convention. Pakistan has signed and ratified the ICCPR, a human rights framework.

The Budapest Convention outlines the types of offences cybercrime laws cover and the procedures they should list. Typically the offences 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.

World over, overbroad legislation is being challenged in court and courts have struck down provisions.

Philippines Supreme Court struck down three clauses from the cybercrime law, Sections 4 c)(3) which pertains to unsolicited commercial communications; 12 which pertains to real-time collection of traffic data; and 19 which pertains to restricting or blocking access to computer data. 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. It also struck down a provision of the law that gives the state power to block content online without a court order.

In March 2014, the **Indian Supreme Court** struck down 66A, a provision of the Indian IT Act "that allowed people to be arrested for 'annoying' or 'offensive' content, including Facebook posts." As reported: "66A was found to be vague and inconsistent with the 8 (constitutionally) permissible grounds for restriction of freedom of expression."

In July, a **UK High Court** ruled that the Data Retention and Investigatory Powers Act as a whole was unlawful. Two UK Members of Parliament had contested the legislation on the grounds that it violated rights and privacy. In particular, it was found to be inconsistent with EU laws and "incompatible with article eight of the European convention on human rights, the right to respect for private and family life, and articles seven and eight of the EU charter of fundamental rights, respect for private and family life and protection of personal data." The government has until March 2016 to come up with a new law.

Conclusion:

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. Any cyber crime bill introduced should be in line with a constitutional framework that safeguards rights. This should be done through an open, transparent and consultative process. Citizens' right to privacy, speech and due process need to be ensured.

Recommendations:

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. This becomes all the more necessary in the absence of data protection and privacy legislation.

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. The data of Pakistani citizens should not be readily shared or handed over - protections and procedures need to be in place. Again, especially since data protection and privacy laws do not exist.

Conclusion:

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.