Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016

By Haroon Baloch

A. Introduction

The National Assembly (NA) of Pakistan has passed the controversial draft of the Prevention of Electronic Crimes Bill, 2016 (PECB)[1] on April 13, 2016. The Government of Pakistan has faced much opposition to this legislation from various sections of the society. Opposition parties including Pakistan Peoples Party (PPP), Pakistan Tehreek-e-Insaaf (PTI), Muttahida Qaumi Movement (MQM) and Awami National Party (ANP) maintained reservations over the draft bill during deliberation process in the NA's Standing Committee on Information and Technology. Bytes for All, Pakistan and its partner organization Association for Progressive Communication already expressed their serious concerns on the Prevention of Electronic Crimes Bill (PECB) 2016 regarding the provisions violating freedoms[2].

PECB aims at restricting the Internet freedoms including freedom of speech, access to information, rights to privacy, peaceful assemblies online and of association. The Bill contains several sections open to vague interpretation, leaving enough room for abuse and misuse by the authorities as well as vests them with complete control of information shared on the Internet and legitimized surveillance.

The Preamble of the Bill indicates that the scope of the law is very wide as it deals with the investigation, the whole process of trial, prosecution and most importantly it talks about the international cooperation, as it provides mechanism for the trial of offences under the law. The preamble also clarifies that it is not only a substantive law but also the procedural law.

B. Objectives

Pakistan ratified the International Covenant on Civil and Political Rights (ICCPR) on June 23, 2010. . After the ratification, Pakistan is bound to abide by its provisions and implement by enacting laws and mechanisms domestically following the true spirit of ICCPR. The Bill directly or indirectly deals with civil liberties enshrined in Articles 17, 18, 19, 21, 22, of ICCPR. The

1 Prevention of Electronic Crimes Bill. (2016, April 13). Retrieved, June 2, 2016, from http://www.na.gov.pk/uploads/documents/1462252100_756.pdf

2 Prevention of Electronic Crimes Bill 2016, yet another story of deception from democracy. (2016, April 15). Retrieved June 08, 2016, from https://content.bytesforall.pk/node/191

PECB 2016 is in the process of being finalized by the parliament, however, several of its Sections are inconsistent with ICCPR. This document in following paragraphs will present a critique on the most controversial Sections of this Bill. If the Bill is enacted as a legislation users of the Internet could be targeted for political and/or ideological reasons and for expressing dissent.

C. Criticism on critical Sections

a. Definitions

The first and foremost criticism on this Bill arises on definitions of used terminologies in Chapter II such as “act”, “access to data”, “access to information systems”, “unauthorized access”, “interference with information system or data”, “critical infrastructure”, “data damage” and “dishonest intention”. None of these terms have been clearly defined and as a result can be interpreted to include many things, and anything should the State choose to criminalise a particular act or person. Following table will help to understand ambiguities and broad terms used in this Bill.

Sr. #	Terminology	As defined in law	Criticism
1.	act	2(a)(i) a series of acts or omissions contrary to the provisions of this Act	A series of acts or omissions according to Bill is the definition of ***act*** where word act is still undefined. It is very confusing
2.	access to data	2(b) gaining control or ability to read, use, copy, modify or delete any data held in or generated by any device or information system	Ability of reading, using, copying, modifying, deleting any data defines broader control over the data with potential of being misused.
3.	access to information systems	2(c) gaining control or ability to use any part or whole of an information system whether or not through infringing any security means	Similar to access to data, this definition allows broad access to information system, does not correspond to the actual meanings.
4.	critical infrastructure	2(j)(i) infrastructure vital to the State or other institutions under constitution whether physical or virtual such that its incapacitation disrupts or adversely affects the national security, economy, public order, supplies, services, health, safety or matters incidental or related thereto; or (ii) any other private or government infrastructure designated by the government as critical infrastructure as may be prescribed under this act.	To our understanding critical infrastructure means the infrastructure, which directly affects the well-being of public in case of its *incapacitation* or *destruction*. Subsection (ii) gives the government Authority to declare anything as critical infrastructure and leaves open to its interpretation.
5.	dishonest intention	2(n) means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred;	Dishonest intention is a vague terminology and the provisions such as intention to create hatred are not dishonest intentions. Again it is a subjective expression and open to

interpretation.

b. Sections 3-8: Unauthorized access with dishonest intention

This Bill covers unauthorized access to information and data in detail in six different sections. Sections 3 to 8 of the Bill criminalise *"unauthorized access"* to information and the vague drafting of these Sections makes them highly susceptible to broad interpretation. These provisions will impede the work of civil society as well as journalists particularly working on accountability issues in Pakistan.

The scope of Sections 3, 4, and 5 is unclear as still there is possibility of criminalizing speech, especially while accessing, copying, and transmission of information or data of public interest by the journalists, bloggers, citizen journalists, whistleblowers, researchers, academics, and non-governmental organizations without permission. Investigative journalists and independent bloggers, on day-to-day basis deal with information shared by their sources or whistleblowers secretly and intentions are not dishonest but to unveil the facts, expose corruption or mismanagement in the best public interest. Therefore, protection of their sources is very important because everyone has the right to access information.

UN Special Rapporteur on the promotion and protection of freedom of expression David Kaye in his report to UN General Assembly in 2015 stressed on the need of protection of sources and whistleblowers and called on states: "When the right and the restriction clash, as they are often purported to do, Governments and international organizations should not adopt laws and policies that default in favour of the restrictions. Rather, laws should favour disclosures of information in the public interest[3]."

Sections 3 to 8 include *"dishonest intent"* as guidance for accusing for an offence, which is a vague terminology and is defined with a very broad scope in Section 2(p), which reads as: *"Dishonest intention means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred"*. All these are very subjective terms and leave much room for the government to interpret as it wants to. Likewise, it is difficult to measure someone's intention.

Similar criticism also applies to sections 6, 7 and 8. These provisions in addition to 3, 4 and 5 talk about accessing, copying, transmission or interfering *"critical infrastructures"* with dishonest intent. Again the term critical infrastructure is defined very broadly under Section 2(j) (ii). It says: *"Any other private or Government infrastructure designated by the Government as critical infrastructure as may be prescribed under this Act."* Such a broad definition allows the government to declare anything as critical infrastructure, which it deems to. We strongly urge the legislators to revisit all six provisions because they are still inconsistent and disproportionate with global access to information regime.

3 Kaye, D. (2015, September 8). Report on Protection of Sources and Whistleblowers. Retrieved June 07, 2016, from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361

c. Section 9: Glorification of an offence and hate speech

> *"Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence and the person accused or convicted of a crime relating to terrorism or activities of proscribed organizations shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to 10 million rupees or with both."*

Section 9, despite rigorous deliberations of the Internet rights activists with NA sub-committee on IT has been kept in the Bill passed by the national assembly. A few minor changes have been introduced but still its scope is not narrowed down according to global standards on freedom of expression. For example, if implemented, it will suppress any sort of debate on issues of public interest including national security, terrorism or about an accused or convicted in crimes such as in cases of Shafqat Hussain because this section criminalises all types of expression, which is glorifying an offence. Merely specifying this section to "*crimes related to terrorism"* and "*activities of proscribed organizations"* will not resolve our apprehensions.

If Section 9 is read with section 10, its implications are worst because such expression can very easily be interpreted as *"coercing, intimidating, creating a sense of fear, panic or insecurity in the government or the public or a section of the public or community or sect or creating a sense of fear or insecurity in the society and/or advance inter-faith, sectarian or ethnic hatred"*. This will be tantamount to cyber-terrorism now and punishable with 14 years of prison or 50 million rupees fine or with both. Recently, an increase in sentencing harsh penalties is being witnessed for expressing, sharing or accessing material related to religious hate. In two different cases, two Shia Facebook users, Saqlain Haider[4] and Rizwan Haider[5] were sentenced for 13 years imprisonment by Anti-Terrorist Courts. Rizwan was convicted under charges for just clicking on hate content. In both the cases, people took on Twitter and Facebook against harsh penalties and criticized the courts. If Section 9 is implemented on such situations, public criticizing the decisions of courts will be interpreted as *"glorification of offence"* and would definitely be silenced.

d. Section 10: Cyber-terrorism offence

> *"Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to: a) coerce, intimidate, 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) advance inter-faith, sectarian or ethnic hatred, shall be punished with imprisonment of either description for a term which may extend to 14 years or with fine which may extent to 50 million rupees or with both."*

Our concerns on this Section from the day first have been the same that this section will have serious implications over the exercise of political expression and campaigns online, which can potentially be seen as an attempt to "*create a sense of fear, panic or insecurity in the government*

4 AFP. (2015, November 23). Man jailed for 13 years for Facebook 'hate speech' - The Express Tribune. Retrieved June 03, 2016, from http://tribune.com.pk/story/996881/man-jailed-for-13-years-for-facebook-hate-speech/

5 AFP. (2016, March 04). Man Jailed for 13 Years Over Facebook Post. Retrieved June 08, 2016, from http://newsweekpakistan.com/man-jailed-for-13-years-over-facebook-post/

or the public or a section of the public or community or sect or create a sense of fear or insecurity in society". This would essentially mean that dissent and freedom of assembly and association online could be targeted in the name of public order. In an age where human rights defenders and journalists are increasingly using the Internet and social media for rights' promotion, dissemination of information and advocacy, their legitimate work and expression may be construed as threatening order and creating chaos. Citizens supporting such political campaigns online can be charged under cyber-terrorism offence with up to 14 years of imprisonment or 50 million rupees fine or with both. If this section was in effect, online campaigns by rights activists such as #ReclaimYourMosques led by Jibran Nasir against fanatics like Maulana Abdul Aziz who denied condemning of Peshawar incident where over 132 innocent school children were killed, would not be possible[6]. In Section 10(b), word "*discord*" is replaced with "*hatred*", which although conveys clear meaning, however, incitement of hatred is being confused with the act of terrorism. Also in Pakistan no legal mechanism is available to deal with inter-faith, sectarian or ethnic hatred. We demand to explicitly define the mechanism for ascertaining certain content that tantamounts to incite hatred or violence.

We believe that cyber-terrorism and cyber crimes are different domains and must be dealt under different laws. Dealing both under PECB would result in confusion.

e. Section 13 & 16: Criminalising encryption and anonymity tools

> Section 13: Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent 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 six months or with fine which may extend to fifty thousand rupees or with both.
>
> Section 16: Whoever unlawfully or without authorization changes, alters, tampers with or re-programs unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving information shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

Use of technologies that enable encryption and anonymity are very important in digital age where mass surveillance is compromising the right to privacy of citizens in general and of vulnerable communities in particular. In the context of Pakistan, such technologies are very relevant as well. More particularly, the Bill criminalises the production, distribution and use of encryption technology under Sections 13 and 16. This provision compromises freedom of expression and privacy of individuals. Especially when commenting on political, religious and social issues that may be controversial, persons need the comfort of anonymity and encryption. Whistle-blowers, human rights defenders, and journalists in Pakistan as such work in very dangerous and

6 Rezwan (2014, December 21). Pakistan Say #ReclaimYourMosques From Radicalism in Rare, Bold Protests. Global Voices. Retrieved April 17, 2016, from https://globalvoices.org/2014/12/21/pakistanis-say-reclaimyourmosques-making-a-rare-bold-statement-against-taliban-apologists-and-extremists-everywhere/

challenging circumstances, by denying them access to encryption, their data and sources would become vulnerable and they may be subjected to surveillance.

Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye in his annual report for the 29th session of UN Human Rights Council called on the States to "adopt policies of non-restriction or comprehensive protection, only adopt restrictions on case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education".[7]

In Section 13, we believe that provisions of *"using information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence"* will allow the government to restrict programmers and techies assisting in the creation of encryption tools. In essence, this prevents and penalizes programmers, coders and techies assisting in the creation of encryption tools, which can have a stifling effect on secure communication for those dealing with controversial issues in their profession. Similarly, provisions in Section 16 can potentially be used to criminalise the production of Internet censorship circumvention tools such as proxies or TOR enabled browsers for anonymity.

f. Section 18: Offenses against dignity of natural persons

> Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extent to one million rupees or with both: Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under the PEMRA ordinance 2002 (XIII of 2002).

Section 18 restricts people from transmitting or publishing of information online. Such information could be of public interest, but under this Section can be interpreted as intimidating or harming the reputation or privacy breach. This is again an inconsistent section with global standards on freedom of expression. Human Rights Committee in its general comments on Article 19 of ICCPR urged: "States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases[8]."

As a real life example, we can recall the case of former Interior Minister Rehman Malik and member national assembly Ramesh Kumar Vankwani where they were forced by other passengers to be offloaded from the plane for delaying flight[9]. A mobile video of the scene was

7 Kaye, D. (2016, May 22). Report on encryption, anonymity and freedom of expression. Retrieved June 06, 2016, from https://freedex.org/encryption-and-anonymity/

8 General Comment 34: Human Rights Committee. (2011, September 11). Retrieved June 07, 2016, from http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

9 Dawn. (2014, September 16). Passengers expel Rehman Malik, PML-N MNA from flight over delay. Retrieved June 07, 2016, from http://www.dawn.com/news/1132305

distributed through social media, which went viral ending up with mainstream media coverage. Obviously, this was public interest information, however, if this section was in effect at that time, owner and distributor of the video could have been tried for harming the reputation of minister. It is understandable that an exception for licensed broadcast media is given in Section 18, but that is limited to airing such content from televisions or radio stations. However, this Section will be applicable to all licensed media if they will broadcast the same content through their websites or social media.

g. Section 21: Cyber-stalking

Cyber-stalking, cyber-bullying or online harassment has emerged as a real challenge in recent years, especially in the context of gender and minors. Online harassment of women has been an increasingly reported crime in Pakistan, and there is a need of an effective mechanism to deal with this issue. However, we have apprehensions on the language and scope of the Section 21. For example, Section 21(d) is about *"taking a photograph or making a video of any person and displaying or distributing it without his consent in a manner that harms a person"*.

Such provisions could be threatening for professionals such as journalists, independent bloggers, photographers or videographers and harm their work. Because it is a requirement in modern journalism that newspapers and television channels also web-cast their content. This Section can be problematic in situations such as capturing of photograph(s) of a person by another with no harm intentions and publishing it online. However, if the person deems it was taken to harm him or her reputation and became a source of distress would allow him to file a complaint against the other person. In such cases, as described in 21(3): *"The aggrieved person may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section(1) and the Authority, on receipt of such application, may pass such orders as deemed appropriate including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data."*. Clearly, this Section includes implications, among others, the censorship of legitimate expression. Therefore, we strongly urge revisiting Section 21 with special attention to 21(d) and unnecessary provisions in the name of cyber-stalking should be removed.

h. Section 34: Unlawful on-line content

> 1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to any information through any information system 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, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.
> 2) The Authority may, with the approval of the Federal Government, prescribe rules for adoption of standards and procedures for exercise of powers under sub-section (1).

> 3) Until such procedure and standards are prescribed under sub-section (2), the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act.

This Section is a clear example of legitimizing online censorship, and against the true spirit of a law. Pakistan Telecommunication Authority, a regulatory body that works directly under Ministry of Information Technology and Telecommunication, is being given a blanket authority to interpret the Article 19 of the constitution of Pakistan. Sub-section 34(1) replicates the "so called" reasonable restrictions imposed on freedom of expression in Article 19 of the constitution and provides authority of interpretation to PTA, which means the role of reviewing the law is being transferred from the Supreme Court to the regulator. A due process of reviewing the restrictions is clearly missing in this case, and is contrary to global standards and basic requirements for a law. This will not only permit the government to censor dissent from within the country, but will give a legal cover to block anything conflicting according to this law coming from foreign sources. Various prestigious international news websites and online research journals frequently write and produce content where they will criticise Pakistan's foreign and defense policy, or they keep exposing the systemic corruption in Pakistani democracy, for example recently released Panama leaks by the International Consortium of Investigative Journalists. If PECB becomes law, the government will be legitimized under this Section to block such websites in Pakistan, which will violate citizens' right to access information. In case of PTA, multiple Right to Information requests were submitted by Bytes for All, Pakistan seeking information of blocked content in Pakistan, but to no avail. It is also fact that PECB does not offer any redressal mechanism to, which petitions of power abuse by PTA or investigation agencies could be filed. In this situation, this section can be very dangerous for citizens' right to freedom of expression.

i. Section 39: International Cooperation

Section 39 will permit the Federal Government to extend cooperation to foreign governments, agencies, and international organizations with regards to collection, preservation and transference of 24 x 7 network information and digital data of Pakistani citizens collected in forms of audio, video, images, text, or any digital format without any permission from the Court. This section is highly controversial in the context of citizens' privacy. With the proven facts revealed in its report[10] by the Privacy International, the intentions of Section 39 are clear that the government is legitimizing all such practices where it was already sharing personal data and information of Pakistani citizens with foreign agencies running controversial surveillance programmes. "Pakistan has participated in and has been subject to, including programmes operated by the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ)": the report disclosed.

10 Tipping the scales: Security and surveillance in Pakistan. (2015, July). Retrieved June 6, 2016, from https://www.privacyinternational.org/sites/default/files/PAKISTAN REPORT HIGH RES 20150721_0.pdf

D. Analysis

Several provisions in Sections 14, 15, 16, 17, 22, 23, 27, 28, 29, 30, 31, 32, 33, and 45 of the legislation have vague, ambiguous and broad scope which have been drafted loosely leaving too much room for interpretation and provide for broad punitive measures. In an environment where the rule of law is as such compromised such legislations will pave the way for rights' abuse. These complications will ultimately add in backlogs of cases adding to the strain of trial courts as well as the apex court. Similarly, the complex and ambiguous language would also create great difficulties for the common person using the Internet as there is an uncertainty of what acts would constitute an offence.

The PECB 2016 is also problematic as suspects accused of a cyber crime are assumed guilty until proven innocent. Given that the law creates new offences, increases the gravity of existing offenses and has increased penalties in terms of imprisonment and fines. It is very much necessary that legislators review this legislation with care and caution.

E. Conclusion and recommendations

While the stated objective of the Bill is to counter ICT driven crimes in the country, but most of the provisions aim at shutting down the free exchange of expression and opinion on the Internet. The Bill must be redrafted explicitly to address crimes and not criminalise expression and associated fundamental rights. In light of the analysis above, Bytes for All, Pakistan and Association for Progressive Communications recommend the legislators, policymakers and the government of Pakistan that:

1. Respect the global standards including ICCPR and ensure that supremacy of fundamental rights, including freedom of expression, right to information, freedom of peaceful assembly and association and right to privacy is not compromised in this Bill;
2. Redraft the Bill using clear and explicit language, and avoid subjective terms such as glorification of offense, coercing, creating a sense of hatred, etc. Such terminologies leave substantial space for the government to interpret according to its needs. Moreover, the terms should be defined with limited and distinct scope;
3. Encourage access and disclosure of public interest information ensuring protection to sources, whistleblowers, journalists, bloggers, and researchers;
4. Appoint and set up a strong, independent and well-resourced privacy commission;
5. Extend the National Commission for Human Rights' role and responsibility to monitor and evaluate law enforcement institutions' working/ operations for better transparency and accountability.
6. Develop an action plan that ensures that the interpretations and implementation mechanism for the Bill includes experts and expertise on digital rights. This should include resource allocation and planning for capacity building of judiciary, lawyers and law enforcement institutions including awareness raising of citizens.

7. Several provisions of the Bill heighten punishment for supposed acts of crime, which may extend up to 14 years of imprisonment and 50 Million Rupees in fines. Such harsh punishments violate the rule of proportionality and will have a chilling effect on rights and freedoms. These provisions should be reviewed and punishments must be reduced in accordance with the rule of proportionality.