To:
The Chairman,
National Standing Committee on Information Technology,
National Assembly of Pakistan

May 6, 2015

Dear Sir,

Citizens and industry professionals would like to draw your attention towards the proposed Prevention of Electronic Crimes Bill 2015.

In its current form, the Prevention of Electronic Crimes bill will adversely impact the IT industry, young professionals, economic investment in the country and constitutional rights and safeguards guaranteed to citizens.

While we believe there is a need to introduce a law to deal with crime, our only request is that the law be formulated in a consultative manner since it is a technical subject, and stakeholder/expert input be sought before it is enacted as law.

As per the official call for public input on the bill, attached are consolidated comments on the proposed law by the Joint Action Committee that comprises citizens and industry professionals. These comments highlight only the major concerns and the most glaring issues. The proposed law, as a whole requires a clause-by-clause analysis and discussion in the presence of all stakeholders: government officials, members of opposition, legal experts, industry professionals, academics and citizens.

We request you to kindly call a public hearing on the Prevention of Electronic Crimes Bill 2015. Through this platform, citizens, industry professionals, academics and legal experts will be able to formally share more input on the proposed law and discuss it in the presence of legislators.

Signed:

Internet Service Providers Association of Pakistan (ISPAK)
Pakistan Software Houses Association (P@SHA)
Human Rights Commission of Pakistan (HRCP)
Pakistan Federal Union of Journalists (PFUJ)
Reporters Without Borders (RWB)
Bolo Bhi
Digital Rights Foundation (DRF)
Bytes For All (B4A)
Media Matters for Democracy (MMFD)
Institute for Research, Advocacy & Development (IRAADA)

Consolidated Comments on: Prevention of Electronic Crimes Bill 2015

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 covered under Pakistan Penal Code (PPC) in any 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.

Moreover, procedural safeguards need to be inserted that uphold and protect citizens' right to privacy, speech and access. Industry must be allowed to operate in a non-stifling environment as per their legitimate right to do business. All powers of authorities set up or empowered under the bill should be subjected to due process and not be overbroad, to curb and keep in check any excesses that may be committed as a result.

TO OMIT:

Section 9: Glorification of an offence and hate speech – This section criminalizes even the '**preparation**' of intelligence even if it is not disseminated. How is this to be determined at all? Then, subsection (a) reads 'glorify an offence or person **accused** or convicted.' This reverses the innocent until proven guilty principle; a crime has not been established. As per this section, 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 ten million rupees or both. Moreover, 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. Why is the need felt only to introduce such a provision for the electronic and online medium whereas on-ground glorification and praise of confessed and convicted murderers goes unchecked?

Section 15: Unauthorized issuance of SIM cards & Section 16: Tempering etc of communication equipment – This makes operators criminally liable whereas this is an already regulated sector and policy directives and existing laws apply. Both offences are already covered under Pakistan Telecommunication (Re-organisation) Act, 1996. There is no need to add this section in PECB and further threaten telecom operators who already have implemented SIM verification policy of Government by spending millions of dollars. PTA under the Telecom Act has tremendous powers to penalize telecom operators for non-compliance of any license conditions and giving more powers to the PTA, FIA and other law enforcement agencies to harass telecom operators is incomprehensible and discourages foreign and local investment.

Section 18: Offences against the dignity of a natural person – This is already covered under Defamation Ordinance, 2002 and Defamation (Amendment) Act, 2004 and penalized under Section 500 and 501 of PPC. 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; neither is any threshold specified. Spamming can easily be curtailed through filters in email inboxes for example, number-blocking options in mobile phones, do not call lists etc. Something that is a source of irritation need not be criminalized allowing people to be thrown in jail. This should be dealt with through policy guidelines and a regulatory framework, not as a criminal offence. Data protection laws need to be introduced to create parameters so that lists of numbers are not swiftly shared or misused for such purposes.

Section 29: This already exists under the Electronic Transaction Ordinance, 2002. This requirement also runs contrary to protecting the right to privacy. Even more so, as such retention would be for a minimum of one year, significantly longer than 90 days envisaged in an earlier draft, and service provider could be required to retain potentially indefinitely, at the discretion of the Authority set up by this law.

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 and curbs media freedom but has huge implications where privacy is concerned. This clause would allow the authority – and in turn the government – 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 – an executive authority cannot be entrusted with a judicial function i.e. interpreting and applying Article 19. As it is, the government and PTA's blocking powers stand challenged in court and this matter is therefore sub judice. The court must be allowed to reach a conclusion in this case; this section must not be used to try and legitimize blocking powers, influence court proceedings or pre-empt a judgment.

Section 43: Prevention of electronic crimes –This clause allows the government to issue guidelines from time to time and makes it an offence if they are not complied with. Problems as have appeared in this law could very well appear with the guidelines, which could be issued without a thorough technical expertise or knowledge of the medium, placing an unrealistic burden on service providers to do something, which may not be practically implementable or possible to do. This also negates the intermediary liability protection offered to service providers in Section 35.

TO AMEND:

(j) Definition of **critical infrastructure** should include private businesses as well, not just government infrastructure

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 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. Open-ended language can easily be misused by the complainants or the Authority. The interpretation of the clauses is not subjected to a judicial process; no already developed jurisprudence would be relied on. An official of the authority would have absolute discretion.

Clause [2] in sections **18, 19 and 21** delegate power to the PTA: the determination of the offence and required action has been left to its discretion. This 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 28: Expedited preservation and acquisition of data gives an "authorized officer" the unilateral and unchecked power to order the provision of data or the preservation of data whenever the officer believes it is "reasonably required for the purposes of a criminal investigation" and there is risk the data may be later inaccessible. While the authorized officer is required to notify a court of such requests, the provision does not require the court to examine the legitimacy of the request or impose any particular safeguards for rights. When combined with expansive data retention requirements under Section 29, this article raises serious concerns about unrestrained government access to private communications. This too should be subjected to a court process and not left to the discretion of an officer.

Section 35: Limitation of liability of service providers - Service providers should not be required to keep investigation or the fact of real-time collection and recording of data

secret indefinitely. The requirement for confidentiality for the first 14 days does not require court's authorisation, and is at the sole discretion of the authorised officer. Secondly, there is no maximum time limit to the extension of such confidentiality that a court may grant. Procedural safeguards must be added.

Section 38: Offences to be compoundable and non-cognizable – Given the excesses committed by investigation agencies in the past, there is little faith that innocents will not land up in jail and be denied bail as they have in various cases – this trend has been noted in FIA cases where bail is deemed as ultimate relief. Currently, Sections 10 and 19 are non-bailable offences. 19 most certainly should not be in this category and given past track record, even 10 should be removed.

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. This will especially impact journalists.

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 and provide detailed reasoning, in writing, for why it is required.

Section 32: Powers of an authorized officer – Sub section (g) gives an authorised officer the power to "require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence." While the provision provides certain guidance on the way such power should be exercised (acting with proportionality, avoiding disruption, seizing data only as a last resort), the powers vested on the officer are very broad and particularly invasive of the privacy of individual's digital communications. Their potential for misuse is extremely high. This is particularly so as the power provided could be used to demand the disclosure of encryption keys, thereby exposing individuals at the risk of disclosure of private data beyond what may be necessary to conduct an investigation.

This will have adverse implications especially on the industry, in terms of data security, and no foreign company would be willing to sign MoUs with a local company if security can be infringed in this manner. This should be removed.

Exercise of powers should be subject to clear checks and balances to curtail misuse since this section contains intrusive powers. Miscarriage of justice and violation of powers should also be accounted for and penalized.

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 Act (as it was in the stakeholder version). Data is sensitive information and how it is seized, handled and preserved needs clear and stringent guidelines.

Section 37: International Cooperation –

The Act gives the Federal Government unregulated, arbitrary powers to share information with international governments/agencies without any oversight.

In sub-section (3) the Act attempts to limit international governments to keep the information confidential or use it subject to some conditions. International governments are neither bound by this Act nor by any such conditions that Pakistan's Government may subject the information to.

In the absence of data protection and privacy legislation, it is 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, to maintain strict checks and balances and avoid violation of privacy.