On September 17, 2015, the National Assembly's Standing Committee on Information Technology and Telecommunications approved the government's proposed Prevention of Electronic Crimes Bill 2015, for a second time. An earlier version was approved in April 16, 2015. Both versions were approved despite reservations expressed by members of opposition part of the NA Standing Committee on IT.

- To track the progress and passage of this bill, read PECB: The Story So Far
- Take a look at the different versions of bills introduced since 2014 and their analyses, in this timeline: Bolo Bhi's Resources on Cybercrime
- Press coverage to date here: In Media Timeline

Below is a markup of the changes made to the latest version approved by the committee. Changes are marked in bold in the second column.

PECB April'15 version	PECB September'15 version	Comments
	A Bill to make provisions for prevention of electronic crimes and matters related thereto.	Statement of Objectives has been added
(e) "authorisation" means authorisation by law or the person empowered to make such authorisation under the law	(e) "authorisation" means authorisation by law or the person empowered to make such authorisation under the law: **Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;**	Proviso added

(j) “critical infrastructure” (ii) any other infrastructure so designated by the Government as critical infrastructure;	(j) “critical infrastructure” ii) any other **private or** Government infrastructure so designated by the Government as critical infrastructure as per rules prescribed under this Act;	Word ‘private’ added.
(r) “information” includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;	(r)“information” includes text, message, data, voice, sound, database, video, signals, software, computer programs, **any form of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996** and codes including object code and source code;	Definition ‘intelligence’ has been removed. Reference to it and the PTA Act has been made in the definition of “information” instead. Word intelligence has been replaced with information in this version, wherever it appears.
	(t) “integrity” means, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;	Definition of “integrity” has been added.
(x) "offence" means an offence punishable under this Act except	(x) "offence" means an offence punishable under this Act except	The age bracket has been raised from seven

when committed by a person under seven years of age or by a person above seven years of age and under twelve, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion.;	when committed by a person under **ten** years of age or by a person above **ten** years of age and under **thirteen**, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion.;	to twelve to ten to thirteen.
(y) "service provider" includes a person who: (iv) provides premises from where or facilities through which the public in general may access an information system and the internet such as cyber cafes;	(aa) "service provider" includes a person who: (iv) provides premises from where or facilities through which the public in general may access **the Internet against payment of charges for the same;**	Sub-clause (iv) has been amended. As per the revised definition, a service provider is one who charges payment for access to the Internet at the premises it is being provided, versus a place where the "public in general may access an information system and the internet." Reference to information system has been removed and requirement for fee/payment to access the Internet for the person/place to qualify as a service provider has been added.
(cc) "unauthorised access" means access to an information system or data without authorisation or in violation of the terms and conditions of the authorisation;	(dd)"unauthorised access" means access to **such information system or data which is not available for access by general public,** without authorisation or in violation of the terms	The portion in bold has been added to the definition.

	and conditions of the authorisation;	
9. Glorification of an offence and hate speech. Whoever prepares or disseminates intelligence, through any information system or device, where the commission or threat is with the intent to:- (a) glorify an offence or the person accused or convicted of a crime; (b) support terrorism or activities of proscribed organizations; and (c) advance religious, ethnic or sectarian hatred	9. Glorification of an offence and hate speech. Whoever prepares or disseminates **information**, through any information system or device, where the commission or threat is with the intent to:- **(a) glorify an offence or the person accused or convicted of a crime and support terrorism or activities of proscribed organizations;** (b) and advance religious, ethnic or sectarian hatred	Reference to "intelligence" has been replaced with "information." Sub-clauses (a) and (b) from have been compounded together The word 'and' has been added to join them.
21. Cyber stalking.- (2) Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment for a term which may extend to two years or with fine up to one million rupees, or with both:	21. Cyber stalking.- (2) Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment for a term which may extend to **one year** or with fine up to one million rupees, or with both:	Jail term has been reduced from two years to one year.

<u>27. No warrant, arrest, search, seizure or other power not provided for in the Act.-</u> (1) Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act:	**<u>27. Power to investigate.-</u>** (1) Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act:	Title of Section 27 has been changed to 'Power to investigate' from 'No warrant, arrest, search, seizure or other power not provided for in the Act.'
<u>30. Warrant for search or seizure.-</u> (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that- (a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorise an officer of	<u>30. Warrant for search or seizure.-</u> (1) Upon an application by an authorised officer... ...offence identified in the application. **(2) In circumstances involving an offence under section 10 of this Act, under which a warrant may be issued, but cannot be obtained without affording opportunity of destruction, alteration or loss of data, information system, device or any other article required for investigation, the authorized officer who shall as far as practicable be a Gazetted officer of the investigation agency enter the specified place and search the premises and any information system, data, device or article relevant to**	Sub-section (2) and a provisio have been added.

the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data or other articles relevant to the offence identified in the application.	**the offence and access, seize or similarly secure any information system, data or other articles relevant to the offence:** **Provided that the authorized officer shall immediately but not later than twenty four hours bring to the notice of the Court, the fact of such search or seizure and the court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.**	
31. Warrant for disclosure of data.- (1) Upon an application by an authroised officer that demonstrates to the satisfaction of the Court...	31. Warrant for disclosure of **content** data.- (1) Upon an application by an authroised officer that demonstrates to the satisfaction of the Court...	The word 'content' has been added to the title of Section 31.
34. Power to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system.- (1) The Authority is empowered to manage intelligence and issue directions for removal or	34. Power to manage on-line information etc.- (1) The Authority is empowered to manage information and issue directions for removal or blocking of access of any information through any information system.	Title of Section 34 has been changed from 'Power to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system' to 'Power to manage on-line information etc.'

blocking of access of any intelligence through any information system. The Authority **or any officer authorized by it in this behalf** may direct any service provider to remove any intelligence or block access to such intelligence, if it considers it necessary….	**The Authority may direct any service provider** to remove any information or block access to such information, if it considers it necessary...	The word 'intelligence' has been replaced with 'information.' The phrase 'or any officer authorized by it in this behalf' has been omitted.
	37. Forensic laboratory.- The Federal Government shall establish or designate a forensic laboratory, independent of the investigation agency, to provide expert opinion before the Court or for the benefit of the investigation agency in relation to electronic evidence collected for purposes of investigation and prosecution of offences under this Act.	New section has been added.
46. Power to make rules.- (1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act. (2) Without prejudice to the generality, of the foregoing powers, such rules may specify:-	47. Power to make rules.- (1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act. (2) Without prejudice to the generality, of the foregoing powers, such rules may specify:-	Sub-clauses (e), (g), (h), (l), (m), (n), (o) have been added.

(a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors; (b) powers, functions and responsibilities of the investigation agency, its officers and prosecutors; (c) standard operating procedures of the investigation and prosecution agency; (d) mode and manner in which record of investigation under this Act may be maintained; (e) working of joint investigation teams; (f) constitution of Computer Emergency Response Team and the standard operation procedure to be adopted by such team; (g) appointment of designated agency having capability to collect real time information; (h) manner of coordination between the investigation agency and other law enforcement and intelligence agencies	(a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors; (b) powers, functions and responsibilities of the investigation agency, its officers and prosecutors; (c) standard operating procedures of the investigation and prosecution agency; (d) mode and manner in which record of investigation under this Act may be maintained; **(e) manner to deal with the seized data, information system, device or other articles;** (f) working of joint investigation teams; **(g) requirements for seeking permission of the Authority to change, alter or re-program unique device identifier of any communication equipment by any person for research or any other legitimate purpose;**	

including designated agency; (i) manner of soliciting and extending international cooperation, and (j) matters connected or ancillary thereto.	**(h) procedure for seeking appropriate orders of the Authority for removal, destruction or blocking access to information under this Act;** (i) constitution of Computer Emergency Response Team and the standard operation procedure to be adopted by such team; (j) appointment of designated agency having capability to collect real time information; (k) manner of coordination between the investigation agency and other law enforcement and information agencies including designated agency; **(l) for management and oversight of the forensic laboratory;** **(m) qualifications and trainings of the officers, experts and staff of the forensic laboratory;** **(n) powers, functions and responsibilities of the forensic laboratory, its**	

	officers, experts and staff; **(o) standard operating procedures of the forensic laboratory to interact with the investigation and prosecution agency;** (p) manner of soliciting and extending international cooperation, and (q) matters connected or ancillary thereto.	

Note on the changes:

The changes made to the current version approved by the NA Standing Committee on IT do not substantially reflect or cater to the input provided to the committee. Other than changes in titles, a word or phrase here and there (that do not alter the meaning or intended application of the sections), the changes remain cosmetic at best.

The major concerns regarding the bill and its provisions remain unaddressed. Recommendations on sections pertaining to powers of authorities, agencies and officers; checks and balance through defined procedures; judicial oversight mechanisms, content and speech restrictions; privacy breaches; all remain unaltered. The bill, in essence, remains as problematic as the version approved before it.