BOLO BHI
Advocacy - Policy - Research

Differences: Government's Proposed
Prevention of Electronic Crimes Bill 2015

Below are sections from the government's proposed bill that are not present, in any form, in Senator Karim Khuwaja's proposed bill.

Chapter I Definitions
(a) "act" includes i) a series of acts or omissions contrary to the provisions of this Act; or ii) causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device, and whether having temporary or permanent impact;
(d) "Authority" means the Pakistan Telecommunication Authority established under Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);
(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;
(f) "authorised officer" means an officer authorised by the investigation agency to perform any function on behalf of the investigation agency under this Act;
(h) "content data" means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;
(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;
(u) "interference with information system or data" means and includes an unauthorised act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data.
(v) "investigation agency" means the law enforcement agency established by or designated under this Act;
(w) "minor" means, notwithstanding anything contained in any other law, any person

who has not completed the age of eighteen years.
(x) "offence" means an offence punishable under this Act except 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.;
(y) "rules" means rules made under this Act;
(z) "seize" with respect to an information system or data includes taking possession of such system or data or making and retaining a copy of the data;
(ee) "unauthorised interception" shall mean in relation to an information system or data, any interception without authorisation;
Chapter II Offences and Punishments
4. Unauthorised copying or transmission of data.- Whoever intentionally and without authorisation copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine up to one hundred thousand rupees or with both.
6. Unauthorised access to critical infrastructure information system or data:- Whoever intentionally gains unauthorised access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine up to one million rupees or with both.
7. Unauthorised copying or transmission of critical infrastructure data.- Whoever intentionally and without authorisation copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine up to five million rupees or with both
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; and (b) advance religious, ethnic or sectarian hatred shall be punished with imprisonment for a term which may extend to five years or with fine up to ten million rupees or with both. Explanation: "Glorification" includes depiction of any form of praise or celebration in a desirable manner.

13. Making, obtaining, or supplying device for use in offence.- Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, primarily 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 6 months or with fine up to fifty thousand rupees or with both.
14. Unauthorised use of identity information.- (1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorisation shall be punished with imprisonment for a term which may extend to three years or with fine up to five million rupees, or with both. (2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.
15. Unauthorised issuance of SIM cards etc.- Whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or other portable memory chip designed to be used in cellular mobile or wireless phone for transmitting information without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine up to five hundred thousand rupees or both.
16. Tempering etc. of communication equipment.- Whoever unlawfully or without authorisation 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 up to one million rupees or both. Explanation: A "unique device identifier" is an electronic equipment identifier which is unique to a mobile wireless communication device.
17. Unauthorised interception.- Whoever intentionally commits unauthorised interception by technical means of:- (a) any transmission that is not intended to be and is not open to the public, from or within an information system; or (b) electromagnetic emissions from an information system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to two years or with fine up to five hundred thousand rupees or with both.

20. Malicious code.-
Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine up to one million rupees or both.
Explanation.- For the purpose of this section the expression “malicious code” includes a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorisation.

22. Spamming.-
(1) Whoever with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without the express permission of the recipient, or causes any information system to show any such information commits the offence of spamming.
Explanation.- “Unsolicited information” does not include:
i. Marketing authorized under the law; or ii. Information which has not been specifically unsubscribed by the recipient.
(2) A person engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe such marketing.
(3) Whoever commits the offence of spamming as described in sub-section (1) or engages in direct marketing in violation of sub-section (2), for the first time, shall be punished with fine not exceeding fifty thousand rupees and for every subsequent violation shall be punished with imprisonment for a term which may extend to three months or with fine up to one million rupees or with both.

23. Spoofing.-
(1) Whoever dishonestly, establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing.
(2) Whoever commits spoofing shall be punished with imprisonment for a term which may extend to three years, or with fine up to five hundred thousand rupees or with both.

24. Legal recognition of offences committed in relation to information system.-
(1) Notwithstanding anything contained in any other law for the time being in force, an offence under this Act or any other law shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to, or through the use of an information system.
(2) References to "property" in any law creating an offence in relation to or concerning property, shall include information system and data.

25. Pakistan Penal Code 1860 to apply.-
The provisions of the Pakistan Penal Code 1860 (XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offences provided in this Act

Chapter III Establishment of Investigation and Prosecution Agency and Procedural Powers For Investigation

29. Retention of traffic data.---
(1) A service provider shall, within its existing or required technical capability, retain its traffic data for a minimum period of one year or such period as the Authority may notify from time to time and provide that data to the investigation agency or the authorised officer whenever so required.
(2) The service providers shall retain the traffic data under sub section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transaction Ordinance, 2002 (LI of 2002).
(3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to six months or with fine up to five hundred thousand rupees or with both.

31. Warrant for disclosure of content data.-
(1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system or data, to provide such data or access to such data to the authorised officer
(2) The period of a warrant issued under sub-section (1) may be extended beyond seven days if, on an application, a Court authorises an extension for a further period of time as may be specified by the Court.

33. Dealing with seized data.-
The Federal Government may prescribe rules for search and seizure and dealing with the information system, data or other articles searched and seized under this Act.

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. The Authority may direct any service provider to remove any information or block access to such information, 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, friendly relations with foreign states, 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 prescribe rules for adoption of standards and procedure to manage information, block access and entertain complaints.
(3) Until such procedure and standards are prescribed, 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.

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.

Chapter IV International Cooperation

38. International cooperation.-
(1) The Federal Government may on receipt of request, extend such cooperation to any foreign Government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act.
(2) The Federal Government may, at its own, forward to a foreign Government, 24 x 7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other Government, agency or organization etc., as the case be in initiating or carrying out investigations or proceedings concerning any offence.
(3) The Federal Government may require the foreign Government, 24 x 7 network, any foreign agency or any international agency to keep the information provided confidential or use it subject to some conditions.
(4) The Federal Government may send and answer requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
(5) The Federal Government may refuse to accede to any request made by a foreign Government, 24 x 7 network, any foreign agency or any international organization or agency if the request concerns an offence which may prejudice its national interests including its sovereignty, security, public order or an ongoing investigation or trial.

Chapter V Prosecution and Trial of Offences

39. Offences to be compoundable and non-cognizable.-
(1) All offences under this Act, except the offences under section 10 and 19 of this Act, and abetment thereof, shall be non-cognizable, bailable and compoundable: Provided that offences under section 15 of this Act shall be cognizable by the investigation agency on a written complaint by the Authority. (2) Offences under section 10 and19 of this Act and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency.

41. Order for payment of compensation.-
The Court may, in addition to award of any punishment including fine under this Act, make an order for payment of compensation to the victim for any damage or loss caused and the compensation so awarded shall be recoverable as arrears of land revenue:
Provided that the compensation awarded by the Court shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation so awarded.

42. Appointment of amicus curiae and seeking expert opinion.-
The Court may appoint amicus curiae or seek independent expert opinion on any matter connected with a case pending before it.

Chapter VI Preventative Measures

44. Prevention of electronic crimes.-
(1) The Federal Government or the Authority, as the case may be, may issue guidelines to be followed by the owners of the designated information systems or service providers in the interest of preventing any offence under this Act.
(2) Any owner of the information system or service provider who violates the guidelines issued by the Federal Government under sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine upto ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both.

45. Computer Emergency Response Teams.-
(1) The Federal Government may formulate one or more Computer Emergency Response Teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan.
(2) A Computer Emergency Response Team constituted under sub-section (1) may comprise of technical experts from private or government sector, officers of any intelligence agency or any sub-set thereof.
(3) A Computer Emergency Response Team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the

information system or data as may be prescribed.