Malik et al LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article Vol. 3 Issue 3, July - September 2019

Deficiencies In Peca And Proposed Amendments To Facilitate Investigating Agencies, Courts And Prosecution; Proper Use Of Electronic Devices For Effective Implementation Of Law

Dr Aftab Ahmad Malik[1] , Mujtaba Asad[2], Waqar Azeem[3]
Professor Faculty of Computer Science Lahore Garrison University (LGU), Pakistan[1]
PhD Scholar, School of Electronics Information & Electrical Engineering
University of Shanghai Jiao Tong, China[2]
Assistant Professor, Department of Computer Science, Lahore Garrison University (LGU),Pakistan[3]
dr_aftab_malik@yahoo.com[1], asadmujtaba@sjtu.edu.cn[2],waqar.azeem@lgu.edu.pk[3]

Abstract:

The purpose of this paper is to analyze and propose amendments in the Pakistan Electronic Crime Act (PECA). It is observed that the Act contains some inherent weaknesses and difficulties due to which some criminals may set free. The investigating agencies, courts, prosecution and the defense attorney formulate a system and work within the ambit of the applicable laws. They derive their strength from the explicit provision of Law and the prescribed procedure. In the case of Electronic Crimes, the forensic evidence, its organization and presentation in the court of law is of pivotal importance. Any deficiency, for example, in procurement of evidence may destroy the entire case of the prosecution in court. The lack of evidence or incorrect procedure of its procurement helps the defense attorney. The judges have to give the verdict keeping in view the well organized and consistent evidence and also under the explicit provisions of law. The central idea of this paper is to make effective modifications and amendments in PECA, as it lacks "proper and soundproof" system for procuring general evidence, forensic and electronic evidence. The paper also focuses on these procedure.

Key Words: Electronic Crimes, Cyber Evidence collection, Electronics Devices

1. Introduction:

The extensive use of digital media and electronics devices has caused an increase in cybercrimes and there has been a need to constitute the law for the protection of rights of citizens. This has adversely curtailed some of the constitutional rights of citizens. The digital forensic and evidence collection is of pivotal importance; it includes computer forensic, incidence response, evidence from mobile, videos, voice biometrics, password recovery and data recovery from demaged devices. The PECA "Prevention of Electronic Crimes Act 2016", was introduced to fight with offenses such as harassment, terrorism infringement of right of privacy of citizens and right to express. According to [1], there have been reservationsin favor and against this bill by a few parliamentarians and the media at the time of its promulgation and making it public. It is reported in [1] that the parliament committee did not appreciate some objections such as sinister, menacing, ominous, creepy and baleful.

The difference between PECA and legislation formerly implemented on the subject of cybercrimes are mostly related to the computer-aided crimes, while the present laws are also relevant to the speeches and actions reflecting criminal behavior. The underline philosophy to implements PECA is to deal with extremist and

terrorist activities such as the killing of our innocent children at Army Public School, Peshawar.

Major Objectives of PECA have been to prosecute hate speech, harassment online, and fighting with terrorism including criminal defamation using I.T systems. We know that the well known top cybercrimes are infringement of privacy, online harassment, hacking personal data of users by illegal means. More effective legislation is the need of the day. A critical discussion has been presented in [2] stressing the need to take necessary measures to make the legislation more effective for implementation. A detailed discussion, procedure and relevant legal points have been raised in [4] and [5] in the context of "Prevention of Electronic Crime Act 2016" and the use of Cyber Space by terrorist organizations.

2. Some Concerns and Reservations about PECA

The complete procedure for collection of evidence must have been a salient feature; which the Act lacks. The unclear provisions in any law are examined on the basis of "Doctrine of Vagueness", which needs the laws to describe clearly the punishable conduct; otherwise, it may be rendered as void.

Vagueness Definition:

Duhaime's Law Dictionary defines "a law which lacks in precision as not to give sufficient guidance for legal debate. Vagueness is a doctrine of constitutional law; and grounds upon which a statute can be found to be inoperative. Every law must be sufficiently clear for the citizens to grasp its import."

According to [2], terrorists use digital tunnels or darknet, which is difficult to trace without adequate expertise; PECA is silent about these terminologies and technologies. Such issues need to be properly tackled and redressed in the revised/amended version of PECA. According to [3], several provisions of PECA are controversial and create the problems due to the restrictions imposed such as potential harm to the right of privacy. According to [6] PECA provides the provision for warrants of retention, search, to have access and for information collection in real-time.

There are concerns of legal experts about certain sections of PECA such as sections 3, 4, 5, 6, 7 and 8 and it is advocated and proposed to make them more effective to strengthen the investigating agencies specially FIA, the prosecution and hence the Courts.

Section 3 prohibits unauthorized access to the information system or data.

Section 4 prohibits unauthorized copying and transmission of data.

Section 5 prohibits interference with information systems or data

Section 6 provides punishment for unauthorized access to critical infrastructure information systems or data.

Section 7 deals with unauthorized copying or transmission of critical infrastructure data.

Section 8 deals with Interference with the critical infrastructure information system or data.

Section 9 relates Glorification of an offense relating to terrorism

Section 10 properly covers the ambit of cyber terrorism envisaged by the above-mentioned sections from 6 to 9.

The sections 31, 33, 34 and 35 provide the procedure for accessing the Data by the investigating officer.

Under Section 37 exclusive powers are entrusted to the PTA (Pakistan Telecommunication Authority) to remove online or block contents of information, this apparently seems contrary to Article 19 of the Pakistan Constitution according to critics. The information to be removed or blocked normally is repugnant to or derogatory to Islamic injunctions, decency, public order or defense of Pakistan. There is provision for the review of the orders of the authority. However, the High Court has the jurisdiction to listen to appeals.

The PECA defines the dishonest intension as quoted below:

"Dishonest Intention" means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence".

The counter-terrorism wing of the Federal Investigation Agency (FIA) has the powers to

summon, detain and investigate the political activists and journalists on the issues of "anti-state activities", propaganda against armed forces, state functionaries and institutions. The PECA provisions must be strong enough to support FIA, prosecution and the court of Law to reach the just decision.

The important factor to be looked into the matter is the intention of the offender. The kind of intention may be that of coercion, intimidation, to create a sense of fear, panic or insecurity. The question arises on how the investigating officer and prosecution should prove the existence of a factor of intimidation, to create a sense of fear, panic or insecurity from the forensic evidence. PECA gives extensive powers to agencies to access private information or Data or to copy and transmit it.

PECA offends the constitutional guarantees of "due process of law" provided in the Pakistan Constitution. The definition of an "act" is not comprehensive, which is defined as a "series of acts". Similarly, the definition of dishonest intention lacks having been defined as similar to legal injury. The words "to create hatred" included in the definition, makes it difficult to prove guilt. Moreover, Cyber-terrorism has not been properly linked with violence and the risk of harm.The prosecution shall have to prove the dishonest intention also when the offender has caused, intimidation, created a sense of fear, panic or insecurity. For this purpose, well qualified and trained personnel are required having expertise in legal, electronics and computer science. A detailed overview of Pakistan's Cybercrime Law has been presented in [12].

3. The Notion of Dishonest Intention

Certain actions committed with dishonst intention are offences. For example, opening a bank account, having unauthorized access to the networks, computer accounts or documents and to impersonate a police officer. The acts of lying , misrepresentation, immoral and unethical behavior, theft at work place by violation of "code on coduct", such as harassment or drug abuse in office; normally such offences are committed with dishonest intetions.

4. PECA Lacks Proper Procedure for Acquiring Evidence

Although the section 31 is related to preservation and acquisition of the Data by the authorized agents, it must be reasonably and properly acquired for criminal investigation. The investigating officer uses randomly his powers what is legally termed as blanket authorization, which lacks checks and balances. The Blacks Law Dictionary defines the Blanket Authorization [16] as a contract letting a party to do an activity with no approval.

This provision is perhaps capable of being used against political opponents. The investigating team may consist of the personnel from the following penal:

- Forensic Specialist,
- High Tech Crime personnel,
- Cyber Security Specialist
- Computer Forensics Lab representative from Computer Crimes unit, Forensic and Technical Services
- Computer Specialist, R&D

5. Important Steps in Digital Evidence Processing

For the purpose of processing the evidence, following procedure should be adhered to in the logical order as per policy and rules of the investigating agency, Evidence Assessment, Evidence Acquisition, Evidence Examination and Reporting. The assessment of forensic evidence is of fundamental importance. As the foresic evidence is fragile and can be demaged or changed, therefore, at the time of acquisition special care must be taken to preserve it with integrity and all contents intact. It ia always recommended to make best bit-by-copy of the original evidence. During the examination of the evidence, we extract, analyse and recover the relevant Data and then legally interpret it after making it logicaly in useful form. Afterwards, we perform activities such as, examination of the partition system, physical extraction, logical extraction of data from drive, extraction of file system and file sizes with their locations, recovery of deleted files, encrypted and compressed data. Final step is the prepreation of written report containing the conclusions and

findings.

The findings must enlist all files with detailed description and relevance to evidence along with those of deleted files, graphics, pictures, hidden files and hidden attributes.

6. Forensic Image MD5 must be Prepared at Scene of Offence

According to [13], The basic way to preserve the evidence is obtaining mirror image of hard disk, which is called forensic image or hard drive clone. It is the bit-to-bit exact copy of the original hard disk obtained from the scene of crime.

This paper highly recommends that the image or clone be prepared at the scene of offence at the time of collection of forensic evidence to avoid future complication in the court.

Technically speaking, MD5 is a versatile method called Message Digest Algorithm. Actually, it is a cryptographic Hash function, which can check and verify that the contents of the file or drive have not been changed. On input of any size it returns the requisite output authenticating the input. "The output from MD5 is a 128-bit message digest value". The following are relevant particulars discussed [14]:

Digest sizes: 128 bit

Block sizes: 512 bit

Rounds: 4

7. Devices where the Criminal Data Resides

There are several ways and means to store the Data and place it. The most useable in practice are the Cloud Storage, Mobile devices like USB, Compact Disk, and other portable storage media, printed material, hard disk (Secondary memory devices), audio and video Disks Photographic images or stored data while communication onto websites using computers, mobile devices, and Networks.

8. National Force for Cybercrimes NR3C

According to [7], the Federal Investigating Agency (FIA) established the National Response Centre for Cyber Crimes in 2007 to fight against the misuse of technology in society. It possesses expertise in IT, digital forensics and Technical investigation. It is providing training to the Police, Judiciary, Lawyers and academia through short courses, seminars and workshops to create proceedings. The protection of recovered forensic information has been an important and debatable issue due to the undefined chain of custody of the information. Unfortunately, no proper procedure has been prescribed in PECA on how to collect and organize information.

The protection of recovered forensic information has been an important and debatable issue due to the undefined chain of custody of the information. been an important and debatable issue due to the undefined chain of custody of the information.awareness. There are a few examples of the areas of forensics used and exploited by offenders, such as legal difficulties arising due to ignorance of investigating officer.

It has been observed that often the embarrassing situations do arise in the court of law merely due to ignorance or lack of knowledge for not following up proper and complete procedure on the eve of collecting information at the scene of offense. There are four important pillars i.e. the court of law, the prosecutor, investigating officer and the attorney of the offender. Any pitfall in the collection of forensic evidence may destroy the case of the prosecution. Most of the time, the investigating agencies and investigating officers do not take the prosecutor in confidence. The prosecutor is also sometimes ill-informed about complete evidence collected and how it was acquired. In the case of naïve evidence and violation of procedure by investigating officer makes the case stronger for attorney of the offender.

9. Acquisition and Preservation of Data for Evidence

In case the forensic information is lying in the hands of unconcerned and incompetent personnel, it is liable to be forged or altered either at the disadvantage to the offender or to save him from the offense and allegations. The percentage of this factor is high. Therefore, the question of acquisition and preservation of Data is extremely important. Following are some

points to observe while collecting and preserving the forensic Data:

- In case of Disks, a bit by bit copy be prepared at the time of procuring it on the scene of offence,
- The reliable chain of custody must exist in the office of Investigating agency who can preserve it with great care and caution.
- In case it is to be sent to the IT Experts, another similar bit-by-bit copy with complete index be prepared. This is what we term as forensic duplication of evidence.
- The copy may be handed over to the experts for evaluation in LAB, while the original documents or Disk shall reside with a reliable chain of custodians.

10. Preparing Clone and Mirror Image of the Hard Disks and a Golden Rule

Technically, the forensic image of the hard disk is termed as mirror image or hard drive clone. It is a pre-requisite for digital forensics proceedings to create an exact digital image of the devices such as fingerprint, hard drive, SSD, USB or other media. We create a unique digital image required for court proceedings so that the authenticity of collected forensic evidence is not challenged.The Golden Rule of digital evidence is that original media should never be changed. Therefore, it is very strongly recommended that the bit-by-bit mirror image (copy) be prepared, the process is called forensic imaging.

It is useful to know the difference between clone and image of a disk or media. The colon can be prepared by using image. The clone is a working and functional copy of the original hard disk, while the image is an “archive” of the disk and can be used to make a bit-by-bit true copy. The procedure for copying the disks has been discussed in depth in [8],[9], [10] and [11]. The digital forensic experts must know what is the appropriate tool is to be used to create the clone or an image; he must have appropriate qualifications and training. When the creation of image is complete any industry-standard tool can be used. A hash generation process looks up the entire zeros and ones which are across the source media. One way is copying Data from one Hard drive to another drive, the drive which is of larger size its blank spaces are filled with zeros after copying data onto it. We may copy Data from drive to a file sector by sector; the authors of this paper don't recommend this manner.

Conclusion

The PECA sections 3, 4, 5,6,7,8, 26 and 27 particularly need revision/amendments while other provisions also need minor revision, where there are pitfalls. The fundamental purpose of the promulgation of PECA was to facilitate certain procedures well defined under digital transformations, because of recent improvements in the innovation and advancement in electronic devices and procedures. The terrorists use digital tunnels or darknet, which is difficult to trace without adequate expertise; PECA is silent about some terminologies and technologies.This aspect and feature must be fulfilled.The investigating officers must be qualified and well trained in the current state-of-art in Internet, Computing, Information Technology and Law. The training facilities for FIA investigating teams may be arranged at the universities having advanced forensic Labs, for Example, Lahore Garrison University Lahore. The legal difficulties arising due to unqualified investigating officers may be minimized by either their replacement with highly skilled and qualified personnel or their training must be a regular feature to properly tackle the well-known Cybercrime categories particulrly Money Laundering, Hacking and Identity theft, violation of Intellectual property rights, Bank Frauds, financial misappropriation and electronic terrorism.

Acknowledgment

The authors are grateful to Mr. Kaukab Jamal Zuberi, Director Digital Forensics Research and Service Center (DFRSC), Lahore Garrison University for his encouragements. The authors also extend the gratitude to Dr Dil Muhammad Former Professor of Law College Punjab Univeristy, Lahore for guidance.

References:

[1]: Farieha Aziz (2018): "Pakistan's cybercrime law: boon or bane?" Heirich Boll Stiftung, The Green Political Foundation and Perspective of Digital Asia.

[2]: Amir Shahzad (2019): "Cyber-Terrorism Law, Implementation and Ways Forward", LGU International Journal for Electronic Crime Investigation; LGUIJECI MS.ID-006 ; Volume 3(2) April – June.

[3]: Eesha Arshad Khan The Prevention of Electronic Crimes Act 2016: An Analysis, LUMS Law Journal Volume 5.

[4]: Zuberi, Kokab Jamal(2019): "Critical Review of Prevention of Electronic Crime Act 2016" (May 7)

[5]: Zuberi, Kokab Jamal. 2018. "Use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation

[6]: Daudpota, Faisal (2016): "An Examination of Pakistan's Cybercrime Law" https://ssrn.com/abstract=2860954 or http://dx.doi.org/10.2139/ssrn.2860954

[7]: www.fia.gov.pk

[8]: Sammons, J. (2015), "Digital forensics: threatscape and best practices". Syngress.

[9]: Gary Hunt, What is a Forensic Image? Best Practices, Forensics https://qdiscovery.com/what-is-a-forensic-image/

[10]: https://capsicumgroup.com/2-key-differences-between-digital-forensic-imaging-and-digital-forensic-clone-and-how-they-can-affect-your-legal-case/

[11]: "How To Make The Forensic Image Of The Hard Drive", https://www.digitalforensics.com/blog/how-to-make-the-forensic-image-of-the-hard-drive/

[12]: Faisal Daudpota(2018),"An Examination Of Pakistan's Cybercrime Law' (2016) Ssrn http://dx.doi.org/10.2139/ssrn.2860954

[13]: Gary Hunt,"What is a Forensic Image?" Best Practices, Forensics.

[14]: Ronald Rivest, "Structure: –MerkleDamgård construction Designers"

[15]: Sarah V. Hart, John Ashcroft ,Deborah J. Daniels, " Forensic Examination of Digital Evidence, A Guide for Law Enforcement; Office of Justice Programs U.S. Department of Justice; 810 Seventh Street N.W.

[16]: https://thelawdictionary.org › blanket-authorization