



## Critical Analysis for Data Privacy Protection in Context of Cyber Laws in Pakistan

Khuram Mushtaque<sup>1</sup>, Kamran Ahsan<sup>2</sup>, Adnan Nadeem<sup>3</sup>, Ahmer Umer<sup>4</sup>

<sup>1,2,3</sup> Department of Computer Science, Federal Urdu University, University Road, Karachi, Pakistan

<sup>4</sup> Department of Computer Science, Mohammad Ali Jinnah University, Karachi, Pakistan

Received: July 17, 2014

Accepted: September 24, 2014

### ABSTRACT

Since the data or information has become an asset of any organizations, therefore revealing, misusing and sharing the personal data of any individual or company are considered as a type of cyber crime. Therefore acts are there in different regions of the world to address this crime. The countries where acts are approved need to improve it by indulging technology and providing the awareness to their citizens and organizations. On the other hand, the countries where no such acts have taken place are maximum vulnerable in this context, so they need to take guidelines of different acts around the world and design a comprehensive act for their regions to prohibit this type of crime and penalize the culprits appropriately.

**KEY WORDS:** Data Privacy, Digital Forensic, Cyber Crime, Cyber Laws, Information Security

### INTRODUCTION

In the field of Cyber Crime, Pakistan is reckoned in those countries where the cyber crimes is counted and taken seriously as other types of crime. There is the need to data privacy and protection act because this law will be capable to safeguard the individual's information and confidentiality of clients where transaction are made over some network, collecting, storing, retrieving and disseminating of individual's data.

Employees of any organization are considered the most vulnerable segment in cyber security. <sup>[1]</sup> In June 2010, media reported that secret data from Prime Minister Secretariat was leaked and stolen by two contractually appointed employees of P.M office. The administration could not detain the offenders and no any legal proceedings could be raised against them. Same is the status of commercial and corporate organizations sector where it used to be declined to report and put on trial the offender employees owing to missing of cyber crime related regulations and laws. <sup>[2]</sup>

Apart from individual level, the potential impact that data leakage can have on a country's national level as well and it can be wide reaching and potentially catastrophic. One of the most recent breaches came up when in January 2013 South African companies' security measures has released a trove of South African personal information to the Internet. This incident saw as much as 700000 records exposed. <sup>[3]</sup>

Similarly, on 17<sup>th</sup> and 19<sup>th</sup> April 2011, a hacker penetrated and successfully browsed the personal information record of around 77 million Play Station Network account. Sony Company announced it on 26<sup>th</sup> of April, after a week of intrusion occurred. Although it is rational that they acquired services of external forensic team and it prolonged to conclude the private information had been recovered, given the Easter break. <sup>[4]</sup>

In general privacy and protection field, According to Article 14(1) of the 1973 constitution of Pakistan "The pride of anybody and, subject to law, the home privacy, shall be unbreakable". But specifically, the law for data privacy and protection is still missing in the constitution of Pakistan. <sup>[5]</sup>

The hindrance in Pakistani endorsement of legislation of data privacy and protection increased uncertainties that it might sidetrack outsourcing business inside the European Union to the latest Eastern European Member States, or to other countries that offer sufficient standards of safeguarding for individual's data by means of lawmaking or other similar ways.

An Electronic Data Protection Act draft comprising subsets of European Union standards on data protection is presently under consideration. A drafted act came up as some hope in year 2005 when an act named as Electronic Data Protection Act was put in front of the legislators for approval.

---

\*Corresponding Author: Khuram Mushtaque, Federal Urdu University of Arts, Science and Technology, Karachi  
Khuram.mushtaque@gmail.com, +923332435415,

### **Pakistan Context: Electronic Data Protection Act 2005**

In the first section of this act, it is explained that this act is drafted to be effective to the entire Pakistan. Second section of this act elaborates that the gathered data shall be processed in the prescribed manner or according to the instructions given by data controller as long as any violation is performed. Third section of this act briefly highlights the rights of data provider of being informed and consented regarding processing of the provided data.

In section four, it is directed to provide electronic data security to data subject and assure minimum chances of risk. Section five of this act deals with the disclosure or dissemination of the gathered data and ensures that the data will be disclosed only to the extent of contract between data subject and processor. Sixth section highlights the powers and functions of the federal government such as preparation of ethics and certain code of conducts, verification of compliance of codes, interaction with different relevant organizations and agencies etc. Section seven describes the types of complaints and crimes occurred in this context. It also illustrates the role of judges and court of law in such cases.

In the conclusive section eight of this drafted act, some temporary and misc provisions are given to the involved parties of the agreement pertaining to data privacy and protection issue.<sup>[6]</sup>

### **Cyber Security Council Bill 2014**

In Pakistan, a senator Mushahid Hussain Syed presented a bill titled as Cyber Security Council Bill 2014 in the Senate of Pakistan On April, 14 2014.<sup>[7]</sup>

In that bill it is asked to design a council which will be responsible to engage in cyber security related issues. In that bill, the jobs and suggested authorities of that council are also defined in detail. The tasks that will be given to the council will include drafting of the policy and guidelines targeting all the sections of the society to protect them against the severe state of cyber related insecurities both locally and globally.

The bill also stressed to provide the facility of communication between the bodies of government and private sector, academic world, civil society, experts of field of cyber security and also to build up a vision of 10 and 20 years.

This bill of a private legislator presented in Senate of Pakistan tells the story behind the seriousness of Government towards the cyber security related issues. However, government may consider this bill of 2014 to implement in the country level after getting it approved and making a part of the law of Pakistan.<sup>[8]</sup>

### **International Context**

Human Rights Universal Declaration in article no. 12 and United Nations International Covenant on Civil and Political Rights in article 17 have attested the privacy right in this context.<sup>[9]</sup>

A specific set was outlined by European legislations regarding standard and rights for the conduct of private data, in any case of whether that data is stored in private or public.<sup>[10]</sup> In U.S, the lawful custom is further linked with legalizing the data that was collected by the federal government.<sup>[11]</sup>

In the light of 1998 act of United Kingdom regarding data safeguarding, it is explained that confidential data must be fairly and legitimately processed by any organization.<sup>[12]</sup>

The European Commission has highlighted and identified few countries that supply the points of data security reckoned to be sufficient and similar with the European Union levels such as Australia, Argentina, Switzerland, Canada, Jersey and Israel etc.<sup>[13]</sup>

### **Existing Worldwide Acts: Critical Analysis**

In present scenario India does not have any particular legislation that would protect privacy rights of every individual. But the information Technology Act 2000 and amendment Act of 2008 under section 43A says that a business body that possesses handling or dealing with some receptive data or information; and that is careless in implementing and preserving logical security practices and results in illegal loss or illegal expand to any person, in that case that corporation might be declared legally responsible to pay damages to the affected person.

Privacy rights in Constitution of India have recognized under fundamental rights but in the name of the development of E-Governance lot of personal information is misused by some agencies. Ex-“E surveillance projects such as Adhar or UID, National intelligence grid (NatGrid) crime and criminals tracking networks and systems (CCTNS), central monitoring system (CMS) are not supported by any legal frame work.<sup>[14]</sup>

According to a report presented on 17 August 2011 and that was commissioned by the Equality and Human Rights Commission; Laws of U.K could not sustain privacy rights of individuals and should be modified. This report also stated that the Regulation of Investigatory Powers Act and The Data Protection Act are puzzled with breaches and negations and these acts are not able to easily explain to the citizens that what had happened to their private information and what they are supposed to do if that private information is mistreated."

In Data Protection Act individuals rights are given against the utilization of their individually specialized information and deliver the rules that private data possessing organizations in need to stand. In this act, telecom companies are allowed to intercept the communications in many cases and law enforcement agencies can also force telecom sectors to handover them the private and confidential data to them without the consent of relevant customers.<sup>[15]</sup>

In January 2012, European Commission revealed its draft data protection Regulation (Regulation), with the intentions to revise and complement data security law of European Union. Though, in September 2013, the draft was debated hotly with the European Parliament presently considering over 3000 proposed changes to that draft. Commission recommended that reporting of data security breaches must be mandatory. It means that Organizations will have to notify the appropriate data protection authority of a violation without unnecessary wait and, wherever possible, it has to be done within the 24 hours after knowing about it. Moreover, they should also make aware the data subjects without too much holdup except the related data safeguarding authority was contented that the data was adequately secured from the access of unauthorized user, for instance by encryption. Data processors would be subject to the still further heavy need to notify data controllers instantly of any data protection break.<sup>[16]</sup>

On 22<sup>nd</sup> October 2013, according to BBC, Critics declared that latest laws for European data safeguarding contain dodges that might cause to be the legislation ineffective. Critics further said that legislators have hardened the earlier draft regulation, designed by the European Commission to assure that organizations no longer share data of citizens of European with another country's authorities, until clearly permitted by law of European Union or by any international accord. Another clause looks for the limiting the profiling of the user, asking organizations to clarify their use of private and confidential data in depth to clients and to request for their permission first.<sup>[17]</sup>

In U.S, no any all-inclusive law exist which regulates the gathering and processing of private data. In its place, protection of data is legalized by various federal and state laws.<sup>[18]</sup>

In the data privacy protection act of Malaysia, the seven principles of the Act are of general basis. It covers personal data protection from all aspects. In order to have a better surveillance on the online personal data collection activities, a tailored made framework based on The Act and Malaysia's perspective is required. This framework is solely designed to monitor the online personal data collection activities in Malaysia.<sup>[19]</sup>

## DISCUSSION

Above given details about data protection acts in different countries of the world shows the significance of data protection acts in the constitution of the country. Every developed country has designed and executed such act in order to strengthen the protection of confidential and private data. In accordance to entire study, it reveals the importance of existence and implementation of data protection act in Pakistan also. Especially when a drafted act of 2005 is already in place and the only requirement is to present that act into the appropriate platforms of the country so that it could be discussed and after that it has to be approved by the government. However, this act of 2005 can be updated after reviewing the critical analysis and flaws of current acts of different countries and addressing in the act of Pakistan to be approved finally. This will be reckoned as obvious advantage for Pakistan because of delaying this process.

The principal dilemma of the countries where data protection and privacy act doesn't exist is that clients' priceless information is being sold to agreed purchasers in very low prices, that results in the theft of data, spamming, scams and theft of the identity since there no any law exist to penalize those offenders who pinch the individual's data. Similar is in Pakistan, different segments of market are misusing the precious and confidential information of clients without their consent. Especially in telecom sector, fake Sims are being issued by using particulars and information of other people and it makes easier to commit crimes and use those fake identity Sims for communications purpose. The only penalizing act that has been seen by the law enforcement agencies in this context is that they just block those fake Sims but because of no any specific law exist; further penalizing has not been able to take place against the originating sources of that crime.

## CONCLUSION

Since the introduction of technology in different types of industries, Data privacy protection has become requirement of every country now and has been reckoned this as a cyber crime. In order to prevent such crime different mechanism are being adopted such as use of the successful and effective digital forensic. Most of the developed countries has not only drafted and approved the legislations in this regards, but are also implementing it with some effect. However different surveys, workshop and other effective mechanism need to be adopted to

develop awareness amongst the organizations and their clients. This will educate them about their rights and responsibilities about the data. Secondly, incorporating of different technologies in this field will also lessen the violation of such acts.

More alarming situation is in those countries where no any act addressing data privacy protection has been designed. In these types of parts of world, there is no way to penalize anybody or any organization revealing or stealing the private and confidential information to any extent. However, in Pakistan the act is drafted in 2005 but still to be approved by relevant authority, therefore it has not taken place in the constitution as a law yet. There is not only need to perform this type of legislation quickly but also acts of different countries being adopted can be used as guidelines to further improve 2005 act before getting it approved finally.

## REFERENCES

1. Stephen Hinde, "The weakest link" *Computers & Security*, Volum 20, Issue 24, pp 295-301, (2001).
2. Muhammad Tariq, Baber Aslam, Imran Rashid and Adeela Waqar, "Cyber Threats and Incident Response Capability - A case study of Pakistan", 2013 2nd National Conference on Information Assurance (NCIA), IEEE, (2013)
3. I.P. Swart, M.M. Grobler and B. Irwin, "Visualization of A Data Leak How Can Visualization Assist To Determine The Scope Of An Attack?", IEEE, (2013)
4. Hanlon, T. 2011. PlayStation Network hacked, personal information of 77 million accounts accessed. Available from: <http://www.gizmag.com/playstation-network-hacked/18501/> (Accessed 23 April 2014)
5. Report, PI releases analysis of privacy issues in Asian developing countries, Chapter: Pakistan, <https://www.privacyinternational.org/reports/state-of-legal-protections-in-asia/Pakistan>, (Accessed 23 April 2014)
6. Electronic Data Protection Act 2005, <http://www.mofo.com/docs/mofoprivacy/PAKISTAN%20Draft%20Law%202nd%20Revision%20.pdf>, (Accessed 23 April 2014)
7. [http://www.senate.gov.pk/uploads/documents/1397624997\\_197.pdf](http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf), [Access: 12-07-2014]
8. <http://www.moremag.pk/2014/04/15/cyber-security-council-bill-presented-by-mushahid-hussain/>, [Access: 12-07-2014]
9. Donald C. Dowling, Jr. White & Case, *International Data Protection and Privacy Law*, White & Case, (2009)
10. Iosif Androurlidakis and Gorazd Kandus, "A Survey on Saving Personal Data in the Mobile Phone", 2011 Sixth International Conference on Availability, Reliability and Security", IEEE, DOI 10.1109/ARES.2011.98, (2011)
11. Chapin, D.A., "A technology perspective on worldwide privacy regulations", *IBM Journal of Research and Development*, IEEE, Volume:53 , Issue: 2, (2010)
12. Stewart Room and Rowe Cohen, "The requirement of the Data Protection Act 1998", Organized by the Institution n of Engineering and Technology E-Infrastructure, Visual Information Engineering and Multimedia Communications Networks
13. Data Protection in the European Union, [http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf), (Accessed 23 April 2014)
14. Mahantesh. B. Madiwalar and Prof B.S. Reddy, "A Critical Analysis of Data Protection Law In India", *Indian Journal of Applied Research*, Volume : 3, Issue : 10, (2013)
15. Reprt: UK privacy laws are fundamentally flawed, report says, <http://www.out-law.com/page-12160>, (Accessed 23 April 2014)
16. Dealing with Data Security Breaches – the future, [https://www.taylorwessing.com/globaldatahub/article\\_dealing\\_security\\_breaches\\_future.html](https://www.taylorwessing.com/globaldatahub/article_dealing_security_breaches_future.html), September 2013, (Accessed 23 April 2014)
17. Critics Condemn new EU data-protection legislation, 22 October 2013, <http://www.bbc.com/news/technology-24622919>, (Accessed 23 April 2014)
18. <http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/>, (Accessed 23 April 2014)
19. Lim Fung Chen and Assoc. Prof. Dr. Roslan Ismail, "Information Technology program students' awareness and perceptions towards personal data protection and privacy", 3rd International Conference on Research and Innovation in Information Systems – 2013 (ICRIIS' 13), (2013)