International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A CRITICAL STUDY ON DATA PROTECTION AND PRIVACY OF CONSUMER

Khune B Shakuntala, Dr. Kuldip Singh

Research Scholar, OPJS University, Churu, Rajasthan
Research Supervisor, OPJS University, Churu, Rajasthan

ABSTRACT

Due to the fact that data and information are now valuable resources for businesses, it is now illegal to disclose, misuse, or otherwise distribute such information. Thus, there exist acts in many parts of the globe to combat this crime. The nations whose laws are upheld have a responsibility to strengthen it by embracing technology and raising public and institutional awareness. But, nations where no such crimes have occurred are the most susceptible in this context, therefore they should draw suggestions from various acts throughout the globe and build a complete act for their areas to ban this sort of crime and suitably punish the perpetrators.

Keywords: Information, Misuse, Technology, Awareness, Businesses

1. INTRODUCTION

India is recognised as a leader in the realm of cyber-crime by nations that treat cybercrime with the same gravity as traditional forms of criminality. There is a need for a data privacy and protection act because such a legislation will be able to protect the personal information and privacy of customers throughout online transactions, as well as during the gathering, archiving, retrieval, and dissemination of such data. In terms of cyber security, an organization's own staff is often seen as its weakest link. The media reported in June 2010 that two contractually assigned workers of the Prime Minister's office had leaked and stolen confidential material from the Prime Minister's Secretariat. There was no way for the government to arrest the criminals or bring charges against them. The same is true in the business and corporate sector, where reporting and prosecuting offenders inside the company was previously rejected due to a lack of cyber crime related policies and laws. The effects of data leakage are not limited to the private sector; at the national level, they may have far-reaching and even disastrous consequences. When South African firms' security procedures failed in January 2013, sensitive personal information about millions of South Africans was leaked onto the Internet. Around 700,000 records were compromised as a result of this incident. Furthermore, between April 17 and 19, 2011, a hacker gained access to the user profiles of almost 77 million Play Station Network accounts. The Sony Corporation made the announcement on the 26th of April, after the hacking had gone on for a week. Given the Easter holiday, it seems sense that they hired an outside forensics team and took some time to determine that no sensitive data had been compromised. In the realm of personal security and

confidentiality, In India, one's "pride" and "home privacy," within the bounds of the law, are guaranteed under Article 14(1) of the constitution from 1973. Yet, the data privacy and protection provision is still lacking from the Indian Constitution. Due to delays in the Indian government's endorsement of data privacy and protection legislation, concerns have grown that the country will divert outsourcing business from the European Union to the newest Eastern European Member States, or to other countries that provide adequate standards of safeguarding for individual's data through legislation or other similar means. Data protection rules from the European Union are being considered in a draught of a new law to secure electronic records. In 2005, a bill with a hopeful name, the Electronic Data Protection Act, was introduced in Congress.

1.1.1 Existing Worldwide Acts:

There is currently no statute in place in India that would guarantee everyone the right to personal privacy. However, according to section 43A of the Information Technology Act 2000 and the Amendment Act of 2008, if a company is in possession of handling or dealing with some receptive data or information and is negligent in implementing and preserving logical security practises and the result is the illegal loss or illegal expansion to any person, the company may be held legally responsible to pay damages to the affected person. Although the right to privacy is protected by law in India, it has been abused by government agencies in their pursuit of E-Government modernization. There is no legal framework to back ex-E surveillance programmes like Adhar or UID, the National Intelligence Grid (NatGrid), crime and criminals tracking networks and systems (CCTNS), or the Central Monitoring System (CMS). [14] The Equality and Human Rights Commission commissioned a study that was released on August 17, 2011, finding that current U.K. law does not adequately protect citizens' right to privacy and recommending alternative legislation. Another finding of the report was that "the Regulation of Investigatory Powers Act and The Data Protection Act are befuddled with breaches and negations, and these acts are unable to easily explain to citizens what had happened to their private information and what they are supposed to do if that private information was mistreated."

The laws that companies in possession of private data must abide by are laid forth in the Data Protection Act, which grants people protections against the use of their personally identifiable information. Without the knowledge or agreement of its consumers, telecom businesses are given broad authority to intercept conversations, and law enforcement authorities are given broad authority to demand the surrender of private and personal data from telecom sectors. [15] The European Commission published its proposed Data Protection Regulation (Regulation) in January 2012 with the aim of updating and expanding EU data security legislation. In spite of this, there was heated discussion about the draught in September 2013 and the European Parliament is now debating more than 3000 suggested amendments to the text. The Commission suggested making it law that each time there was a breach in data security, the incident was reported. This implies that organisations must report the relevant

data protection authorities as soon as they become aware of a breach, and in any case no later than 24 hours after discovering the breach. In addition, they shall notify the data subjects without undue delay unless the relevant data safeguarding authority is satisfied that the data has been effectively safeguarded from the access of unauthorised user, for example, by encryption. An additional onerous obligation placed on data processors would be to immediately alert data controllers of any data protection breach.

According to the BBC, critics have claimed that loopholes in recent European data protection rules render them worthless as of October 22nd, 2013. Critics also claim that legislators have tightened up on the original draught regulation proposed by the European Commission to guarantee that companies will not share data on European citizens with the authorities of any other country unless expressly permitted by European Union law or by an international accord. Another provision seeks to restrict user profiling by mandating that businesses provide comprehensive explanations of how they will utilise sensitive customer information and get express consent before doing so. In the United States, there is no comprehensive legislation that controls the collection and use of personal information. Instead, data protection is codified at the federal and state levels. Under Malaysia's law protecting personal information, there are seven overarching principles. It's comprehensive in its security of sensitive personal information. To more effectively monitor online personal data gathering operations, a bespoke structure that takes into account both The Act and Malaysia's viewpoint is necessary. The main purpose of this framework is to keep tabs on how much personal information is being collected online in Malaysia.

2. DATA PROTECTION LAW IN INDIA

Now that we live in the information era, India may achieve new heights of success in areas such as education, healthcare, and public service delivery. Indians have a worldwide reputation for their diligence and perseverance. Changes in one area of life always have an effect on other others. People in the past only dealt in cash and did not have access to banking services, computers, or telephones. But, in today's increasingly digital world, it's impossible to survive for long without access to basic communications infrastructure like a bank account or Internet connection. Nowadays, everyone needs some kind of electronic payment system, whether it be a credit card, a traveler's check, an email, or some other form of electronic payment. As a result of technological progress and reliance on computers, we can now simply pay our energy and phone bills online and have them delivered to our doorstep with a few clicks of the mouse. On the other side, we're increasingly entrusting our private data to digital platforms, which may be quickly altered in a variety of ways.

For example, if you make a purchase at a store and pay with a credit card, the store will record your payment information and may share it with other businesses for marketing purposes without informing you. This is just one example of how information is passed from one party to another in today's economy. Because of this, it is clear that as internet usage grows, new laws will be required. There is a vast quantity of information available on the

internet for individuals of all walks of life and every imaginable need. As an increase in e-commerce can be directly attributed to an increase in internet usage, it follows that the internet is a truly global phenomenon. The issue here is the lack of regulation, and new laws are being introduced to address this issue by establishing guidelines for the collection, storage, and dissemination of personal information kept in electronic form. Data protection laws are one possible solution to this problem, and they have proven effective in the developed world.

2.1 Historical background of data protection law

In the year 1970, the German federal state of Hysee passed the first data protection laws. Many people were wary of using computers to store and analyse significant amounts of personal data because of Nazi Germany's abuse of records. It's a symbol of how publicly available data gets abused. The law was first enacted in 1973 by the Swedan Nation. The UK government was worried about the effect the council of Europe norms would have on businesses and worked to bring the country up to international standards so that data could be shared across countries. In 1982, it proposed legislation that eventually became the Data Protection Act of 1984. As early as 1995, the European Union passed a rule meant to safeguard people' privacy while handling personal data. U.S. enterprises who have self-certified to the safe harbour framework are protected by this framework, which was defined and created by the U.S. government and is maintained by the U.S. Department of Commerce.

2.2 Why India need data protection

Currently, Indian data is safeguarded under Sections 43A and 72A of the Information Technology Act of 2000; this applies even to data that is transferred outside of India. "The Information Technology Amendment Act of 2008 has started the process of filling the void in our country's data protection regulations." Indian corporations in the IT and BPO industries receive and access all types of personal data and sensitive data's from across the globe, including credit card and medical information, but the changes to Sections 43A and 72A of the IT Act would not be enough to satisfy them. When organisations keep such sensitive data on their computers, the data may be at risk if the hands of their workers. Indian BPOs have had security breaches in which New York City bank accounts were stolen from BPOs in Pune. In another case, a call centre worker in Bangalore sold customer credit card details and stole US$398,000 from British accounts.

Privacy violation: The right to privacy can be divides into four concepts

Information ‘privacy’:

This requires the creation of regulations for the gathering and storage of sensitive data, such as financial records, medical files, and public documents.

Bodily privacy:

Against intrusive operations like genetic testing, drug testing, and cavity research, people's physical selves are a major worry.

Privacy of communications:

This includes the confidentiality and privacy of all electronic and postal correspondence.

Territorial privacy:

Video surveillance and I.D. checks are only two examples of the intrusion into private and public spaces that are becoming more common.

This data protection legislation limits the acquisition, storage, and sharing of private information in ways that are minimally intrusive to individuals. Information about an individual that warrants privacy or security measures.

2.3 Constitutional provisions

While the right to privacy is not explicitly guaranteed in the Indian Constitution, it is included in the list of basic rights found in Articles 19(1)(a) and 21. Nevertheless, the states are allowed to put reasonable restrictions on these rights in accordance with Article 19(2). There is currently no statute in place in India that would guarantee everyone the right to personal privacy. But the information Technology Act 2000 and amendment Act of 2008 under section 43A says that 'a body corporate who is possessing dealing or handling any sensitive data or information, and is negligent in implement and maintaining reason able security practises resulting in wrongful loss or wrongful gain to any person, then such body or corporation may be held liable to pay damages to the person so affected. To add insult to injury, anybody who breaches a valid contract without the other party's knowledge or agreement will now face up to three years in jail and a fine of up to 5 lakh (about $10,750) under section 72A of the Information and Technology Act 2008 (amendment).

3. WILL INDIA'S PROPOSED DATA PROTECTION LAW GUARANTEE PRIVACY AND ENCOURAGE DEVELOPMENT?

How can we ensure that privacy is safeguarded while still encouraging technological advancement and increased productivity? In this article, we look at India's proposed data protection law to see whether it strikes the right balance between privacy and security. Towards establishing the country's first comprehensive legislative framework for data protection, the Indian government submitted the Personal Data Protection Bill, 2019 in parliament in December 2019. This article claims that the law does not adequately protect individuals from damage in the Indian data economy due to privacy concerns. Instead, it suggests a preventative paradigm that increases state intervention to excess. The potential erosion of privacy protections from the state and the consequent rise in compliance expenses for enterprises would be very concerning. The study contends that privacy helps to preserve

other purposes, including free expression and sexual autonomy. A more nuanced understanding of privacy's function in modern society and the costs that result from privacy breaches is necessary for the development of an effective framework for safeguarding personal data. The need of protecting one's private data has grown dramatically over the last decade, but as this article shows, India's privacy law has a long and distinguished history. The majority of the discussion is on privacy breaches and the resulting damages. In 2017, the Supreme Court reversed this line of thinking when it issued its ruling in Judge K.S. Puttaswamy v. Union of India, which established a privacy guarantee in the Indian Constitution. While the court cited a substantial body of precedent in reaching its decision, the absence of a "doctrinal framework" to aid in determining whether privacy is constitutionally protected was identified as the case's major shortcoming.

As a result, the law began to see privacy not as a means to a goal but as an end in and of itself. In addition to its finding that privacy is a constitutionally protected right, the court also categorised informational privacy as a component of that right. This paper demonstrates how this change aligns with the stance expressed by the legislation. Instead than safeguarding informational privacy in light of the consequences that can result from its breach, the law seeks to avoid violations by regulating the ways in which corporations gather and utilise personal data. As such, it mainly concerns itself with controlling data-related activities.

This is problematic for a number of reasons, not the least of which is that the proposed framework is unlikely to provide adequate privacy protection. The bill also significantly strengthens the role of the state in the data economy, dilutes property rights in data, and increases state power to surveil without creating adequate checks and balances. Despite failing to achieve its declared goal of safeguarding informational privacy, this is likely to have negative effects on economic innovation. Part one of this document is a synopsis of the significant events that have prompted the need for a data protection legislation. It sets the bill in the wider context of the privacy debate in India and raises issues with the Puttaswamy judgment's definition of privacy. This study argues that the bill is guided by this revised privacy notion and thus falls short of establishing an appropriately tailored regulatory framework to deal with market failures in the digital economy.

Specifically, Sections 2, 3, and 4 explain why Sections 2, 3, and 4 of the law need to be changed drastically. The first is that it is very unlikely to be successful because of its dependence on increasing consent-based systems for safeguarding personal data. There is a growing corpus of research that shows how technological progress renders traditional disclosure obligations to consumers about the way their data is used more useless. Yet, if people come to rely on these systems, they may be less careful with their data sharing. Second, the bill's proposed preventative structure may result in high compliance costs for private companies. The measure would impose new, stringent compliance rules for the overwhelming majority of impacted enterprises and govern data usage across all economic sectors. Any company, no matter how large or small, will have to pay the same amount to

comply unless they fall under one of the exemption categories. As most companies in India are quite tiny, this poses a significant difficulty. They would find it particularly difficult to meet such stringent compliance standards. In addition, the government will be able to require private companies to provide it access to non-personal data under the terms of this measure. The report suggests that this might impede economic development and creativity in the long term.

The bill's Data Protection Authority design is the third key concern (DPA). This committee will be responsible for enforcing the bill's requirements and developing guidelines for matters including consent methods, data use limits, and international data transfers. The DPA has a broad supervisory jurisdiction since it must supervise several preventative measures imposed on firms, such as security precautions and disclosure rules.

3.1 The Growth of Privacy Regulation and the Bill

The Personal Data Protection Bill, 2019, is part of a long tradition of privacy law in India that has been shaped by both international and domestic trends. Although being unstated in the document itself, Indian courts have recognised a right to privacy as part of the right to life given in Article 21. The Supreme Court's long-standing verdict in Kharak Singh v. State of Uttar Pradesh, in which it found that a right to privacy did not exist under the constitution, meant that the precise nature of the constitutional protection of private was never quite clear.

The government's execution of its initiative for unique biometric identity (Aadhaar) and the ensuing concerns of loss of privacy prompted efforts to clarify the situation.

The spread of digital services in India may be directly attributed to the development of the country's information technology sector and the subsequent telecom revolution that began in the late 1990s. There are two major effects of this. For starters, the proliferation of digital services and platforms has increased the level of interdependence in the nation. Second, the administration has realised that providing services online is a potent tool for accomplishing policy goals like financial inclusion and distributing cash transfers. Using Aadhaar has greatly helped with the second goal. Yet, Aadhaar's widespread use has been heavily criticised for some time. One complaint was that commercial companies were using Aadhaar for customer onboarding as well as social assistance distribution. It was claimed that storing consumer information relating to Aadhaar, such as metadata regarding the location of authentication, was a very intrusive invasion of privacy. One such common argument against Aadhar was that it would allow the government to spy on its citizens far more extensively. Similarly, in 2013, the European Union (EU) introduced the General Data Protection Regulation to standardise and consolidate its prior data protection system (GDPR). 9 The previous framework relied on the European Data Protection Directive from 1995. 10 The fear was that the EU's data protection system would become disjointed as a result of this regulation scheme. After several years of deliberation, General Data Protection Regulation

(GDPR) became law in 2018. The discussion in India was informed by the European Union's attempt to adopt a comprehensive data protection policy.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 is being challenged in the Supreme Court because to the privacy issues that have arisen throughout the discussion around the programme. As the petitions alleged an invasion of privacy, the five-judge bench of the Supreme Court that considered them said it was necessary to establish whether or not such a right existed in the Constitution. In August 2017, a nine-judge panel of the Supreme Court ruled that Article 21 does provide the right to privacy, that the Supreme Court erred in its decision on this issue in Kharak Singh, and that informational privacy is a component of this right to privacy.

4. DEVELOPMENT OF PRIVACY LAW IN INDIA

The proposed data protection framework is faithful to the underlying reasoning of the Puttaswamy case ruling by the Supreme Court of India. The right to privacy is a constitutionally protected freedom that the Supreme Court has determined derives from the freedoms of life and self-determination. The very concept of privacy was seen as having both negative (the right to be left alone) and positive (the right to share one's space with others) connotations (the right to self-development). One's right to anonymity falls under the realm of privacy. In accordance with this right, an individual has the option to share her personal information with others or keep it to herself. So, the foundation of informational privacy is the individual's right to self-determination and control over his or her own information.

That said, the court did make this observation: "Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State."

Even the right to privacy might be curtailed under certain conditions.

1. It is in the state's best interest to limit the freedom because:
2. the limitation is reasonable given the importance of the interest at stake.
3. the law imposes the limitation..

The courts' interpretation of how the requirements of a free and fair digital economy can be safeguarded can serve as a useful reference point when deciding whether or not a particular case involves a right to privacy over that which is claimed exists and would prevail over any legitimate interest of the state. Our Constitution was written with freedom and equality in mind because they are vital to our way of life and the reason we fought for our independence.

1. Processing Personal Data- It is important that personal data be only processed (collected, recorded, analysed, disclosed, etc.) for "clear, precise, and legitimate" reasons. In order to complete anyone's request, we need to gather the data that is absolutely essential.
2. Problematic Exceptions- Information about an individual's life may be processed by the government if doing so is required to carry out the duties of either Congress or a state legislature. Providing services, granting permits, and so forth are all part of this category. The first impression is that it is particularly open to abuse due to its lack of specificity.
3. Right to be Forgotten- The group suggested implementing a "right to be forgotten" for "data principles" (those whose personal data is being processed). This implies that if the original reason for disclosure has passed or the data principal has revoked permission, the data subject may limit or prohibit further publication of their personal data. People in the European Union have used this to have outdated or irrelevant articles about them removed from news websites.
4. Data Localisation- In order to comply with the law, personal information must be kept on Indian servers and transfers to other countries must be protected. Nevertheless, only in India will the processing of sensitive personal data take place.
5. Explicit Consent- There shall be no processing of "sensitive" personal data (such as passwords, financial data, sexual orientation, biometric data, religion, or caste) without the individual's express permission, which takes into account the reason for processing.
6. Data Protection Authority- To "protect the interest of data principals," prevent misuse of personal data, and ensure compliance with the safeguards and obligations under the data protection framework by corporations, governments, or anyone else processing personal data, the committee suggested establishing a Data Protection Authority (Data fiduciaries). The Authority will need to publish Codes of Practices on all of the aforementioned criteria, including the duty on data fiduciaries to undertake audits and ensure that they have a data protection officer and grievance resolution system. When the data protection regime is broken, the Authority may investigate and punish the data stewards accountable.

5. CRITICAL ANALYSIS ON DATA PROTECTION AND PRIVACY ISSUES IN INDIA

We create data nearly every time we do something. Our data sharing and data generation are both intentional. Things like going out to eat, using public transit, and booking a hotel room. There is data uncertainty when the data has high value and several firms are interested in acquiring such data. In today's high-tech society, data has replaced traditional forms of payment. Nonetheless, the data's full potential remains unknown, even with all the information at hand. The value of such data is growing as new kinds of technology emerge and new applications are created.

Currently, India lacks any comprehensive data privacy laws. Existing laws and regulations tend to be industry specific. Related parts of the IT Act, 2000 are reflected in these sectoral laws, which provide guidelines for the collection, storage, and disclosure of personally identifiable information and other sensitive data by Indian corporations.

All throughout the globe, legal scholars are still trying to make sense of this time-honored concept of justice. In light of the urgency of the issue, many governments are requesting and looking for access to data from corporations and individuals. Nevertheless, concerns have been raised regarding issues like where an individual's privacy begins and ends. May the information be required to aid fundamental services, travel, or government interests? Is national security more important than individual rights to privacy right now?

Due to the critical importance of data in modern society, safeguarding it has become a significant burden due to the prevalence of potential security vulnerabilities. To ensure that everyone's personal and business information online is safe, legislation pertaining to data protection must be kept current. Case laws and new legislation are being passed to address various privacy concerns in India; as a society, we learn and change and so do the laws that govern us.

5.1 Concept of Data

Information, as defined by Section 2(1)(o) of the Information Technology Act of 2000, is "a representation of any data, information, ideas, directions, or realities that is being readied or had been set up during any formalised way and which is intended to be prepared, is as of now being handled, or has been handled during any figuring framework or organise and will be in any structure, including PC printouts attractive or any sort of optical stockpiling media, punched car, or other tangible medium."

Such electronic assent system is provided by Digital Locker Authority, which defines "information" as any data maintained inside any electric structure by any open or private specialised co-op like a taxpayer-driven organisation office, a bank, and so on.

5.2 Privacy of Data

The use of various electronic devices and apps has resulted in a substantial increase in the amount of data created during the last few years. Today's businesses get a significant advantage from analysing 'big data,' and they base important decisions on the findings of these analyses.

Although the convenience is undeniable, the essential question is whether or not the user has any say over how his or her personal information is accessed and used by third parties. Safety is the assurance of not being targeted for abuse or humiliation because of who you are. The benefit of security is the freedom from irrational risk, the ability to evaluate the consequences

of a lifetime apart, and the chance to measure without unreasonable obstruction from the general public on matters with which they are not interested.

Safety as a privilege has a long history. One of the concepts in law that has developed from precedent is the notion of an assault privilege, which protects an individual from suffering losses due to tort. Semayne's Case (1604) is one of the first cases to address this issue. This is the procedure followed by the Sheriff of London when entering a residence in order to serve a valid writ. Sir Edward Coke, when recognising a man's claim to protection widely remarked that: the location of most are to him as his house and fortress where his barrier from a physical problem and the ferocity for his rest.

Protection as a concept also developed in England throughout the eighteenth century and is still widely used today. In Campbell v. MGN, the court determined that a disruption in any situation where a reasonable person would expect that their security would be considered would be capable of giving rise to any responsibility, unless such interruption is routinely encouraged.

6. CONCLUSION

Since that technology is used in so many diverse fields, every nation has made data privacy protection a priority—and cybercrime—to boot. Several mechanisms, such as the employment of the effective and successful digital forensic, are being employed to avoid such crime. Most industrialised nations have not only created and ratified the relevant laws, but are also actively enforcing them. The organisations and their customers, however, need to be made more aware via the use of various surveys, workshops, and other effective mechanisms. This will help people understand their legal obligations and freedoms in regards to the information. Second, using new technology in this area will further reduce the occurrence of such wrongdoing. Even more concerning is the situation in jurisdictions where no comprehensive law protecting individual privacy in the digital age has been drafted. There are no legal consequences for individuals or institutions who violate confidentiality in these regions. The legislation was developed in 2005 in India, but it has not yet been authorised by the appropriate government, hence it has not been enshrined in the Constitution. Not only is there an urgent need to pass such legislation, but the 2005 act may be improved by looking to similar laws passed in other nations as models.

REFERENCE

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, Pl 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. Iosif Androulidakis 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)
7. 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
8. Data Protection in the European Union, http://ec.europa.eu/justice/policies/privacy/docs/guide/guideukingdom_en.pdf, (Accessed 23 April 2014)
9. Critics Condemn new EU data-protection legislation, 22 October 2013, http://www.bbc.com/news/technology-24622919, (Accessed 23 April 2014)
10. 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)