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

COPY RIGHT

IJIEMR Transactions, online available on 29th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/171

Title DIGITAL PRIVACY IN INDIA

Volume 12, ISSUE 04, Pages: 1323-1334

Paper Authors

Loshika Sharma

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

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

DIGITAL PRIVACY IN INDIA

Loshika Sharma

Ballb 2nd Year

Student

Prestige Institute Of Management And Research

ABSTRACT

Digital Privacy is a multifaceted concept. In social psychology, privacy is defined As the selective control of access to the self. From an economic perspective, privacyrelates to the disutility from losing controlof and the risk associated with releasing personal information. Enabledby AI and big data technologies, digitalization of personal life and smartapplications extend the conceptualization of privacy to digital privacy.The following provides a review of the privacy research developmentfrom three perspectives—privacy as a fundamental psychological need,privacy as an economic trade-off, and privacy as a technical artefact.

KEYWORDS:- Digital Privacy, Information technology (IT) , artificial intelligence (AI)

INTRODUCTION

Information technology (IT) development continues to push digitization forward. Online platforms, smart devices, andartificial intelligence (AI) applications have influenced many aspects ofpersonal life, including commerce, social networking, transportation,and education. In the era of big data, the automatic collection of Nano level personal data empowers advancements in AI and data mining algorithms that generate unprecedented consumer insights and enablesvaluable personalized services. At the same time, the collection andusage of digital personal data and their negligent handling by onlineplatforms endanger privacy. Privacy violation incidences are frequentlyreported and debated, causing significant privacy concerns and anxiety among consumers of digital services. Therefore, there is an urgentneed for proper management systems and regulatory policies to governprivacy related practices in the big data era.Significant research efforts have been

exerted towards understanding digital privacy from different perspectives. Discussions in the context of ecommerce transactions and online social networking; the antecedents and consequences of information privacy concerns are explored, thus shedding light on the management of customer privacy. Economists have studied the economic trade-off between privacy and the use of online services. In the field of technology, research efforts have focused on understanding the inference of personal information from shared data, to improve the security of information systems, and create algorithms that enable data transactions with-out undermining privacy.

Digital privacy is an interdisciplinary concept. On the one hand, advances in information technology prompt the collection and use of personal data while providing tools to protect and manage privacy. On the other hand, privacy protection extends to protecting both the personal space and psychological independence on the Internet beyond personal data. As digital and online social interactions continue to flourish and because of the increasingly ubiquitous merging and sharing of Nanolevel personal data, privacy issues need to be handled appropriately to protect users, while simultaneously empowering the development of the digital economy. A systematic conceptual framework is thus needed to facilitate interdisciplinary research on digital privacy and form an overarching research agenda to empower digital privacy management. This paper develops an ontology of digital privacy combining behavioral, economic, and technical perspectives, based on a comprehensive yet concise review of extant research on digital privacy.

DIGITAL PRIVACY – TOWARDS AN ONTOLOGY

Based on the review of previous research, an ontology of digital privacy is proposed , considering the psychological, economical,And technical aspects of privacy issues in digital economy. Digital privacy is defined as the selective psychological and technical control ofAccess to the digital self in the form of online profiles, personal data,And digital assets. The proposed ontology reflects the cumulative body of knowledge on privacy issues in the digital world and exhibits theLogical relations between concepts.Five core concepts emerged from extant academic discussions aboutDigital privacy: digital

privacy, personal boundary management, personal data management, privacy concern, and privacy coping.At the centre of digital privacy is the need for an individual to differentiate oneself from the social environment for establishing and maintaining an intact self-concept and individuality—the personal boundary management process. In other words, personal boundary management defines the self as a unique individual and privacy claim.Digital technologies create an individual's digital representation in theVirtual space. With the development of digital economy, this digital representation evolved from being a collection of personal data (personalData management needs) to being a integral part of the self-concept—the Virtual self. In the digital economy, individuals virtually inter-Act with a variety of peers in the contexts of online communities, e-Commerce, online services, and online social networks with their digital identities. Such online social interactions blur the natural boundariesThat help individuals to control the adopted identity and maintain self-Concepts . For example, the proliferation of instant communicationTools adopted in working situations leads to the increasing overlap ofwork and family subsystems, resulting in greater work-family conflicts. Effective personal boundary management enables individuals to demarcate boundaries in their work and nonwork roles. Personal boundary management governs six sub-concepts in two layers, and personal data management governs five sub-concepts. While the concept of personal data management concerns primarily the interaction between platform owners (i.e., service vendors) and users, digital privacy directly relates to personal boundarymanagement in all types of social interactions, covering personal data management as a core subdomain. Lack of control in personal boundary management results in privacy concerns, which induce privacy coping effort. Platforms empower/endanger personal boundary management by designing and implementing technical instruments that form the environment for privacy coping behaviour. Privacy regulation governs thesetting of platform policy that informs the design of technical instruments. Accordingly, nine relations are extracted and the premises governing these relations are discussed .

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

ofonline platforms. These platforms

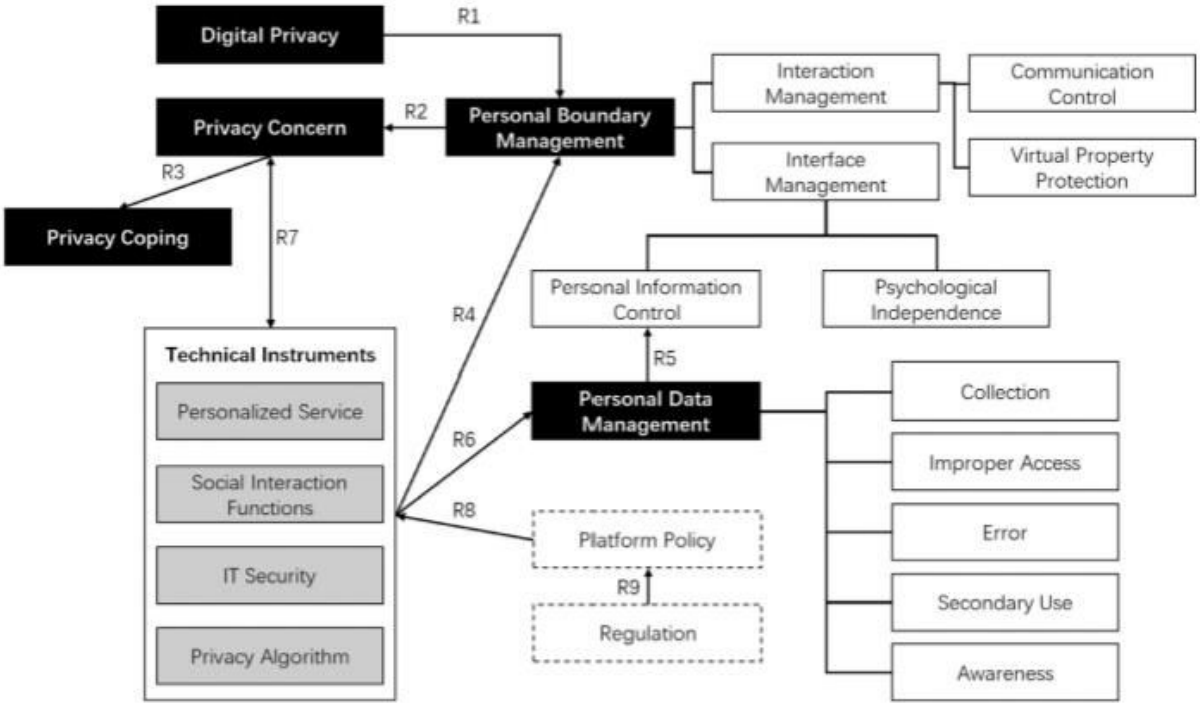

Fig. 1. Digital privacy ontology.

MANAGING PRIVACY ON DIGITAL PLATFORM

The digital privacy ontology discussed here provides an overarching framework for understanding issues related to privacy in the digitaleconomy. It decomposes privacy into sub-concepts that drive individuals' online behaviour and, more importantly, clarifies and highlightsthe roles of technological artefacts, platform governance, and regulations policies in the process of digital privacy management. Digital privacy discussions centre on the creation, evolution, and management (e.g., e-commerce, social networkingservices, and online financial services) should address digital personaldata protection issues, and they should also orchestrate the technicalenvironment for online participation so that privacy concerns are minimized. Recognizing the role of digital platforms and informed by thisontology, the boundary resource perspective is proposed as a valuabletheoretical lens for unifying multi-disciplinary discussions and under-standing privacy management practice in the digital economy that centre around online platforms fuelled by personal data.

undetermined you can be targeted for a campaign aimed at influencing your voting. The simple nature of human psychology makes you vulnerable to such manipulation.

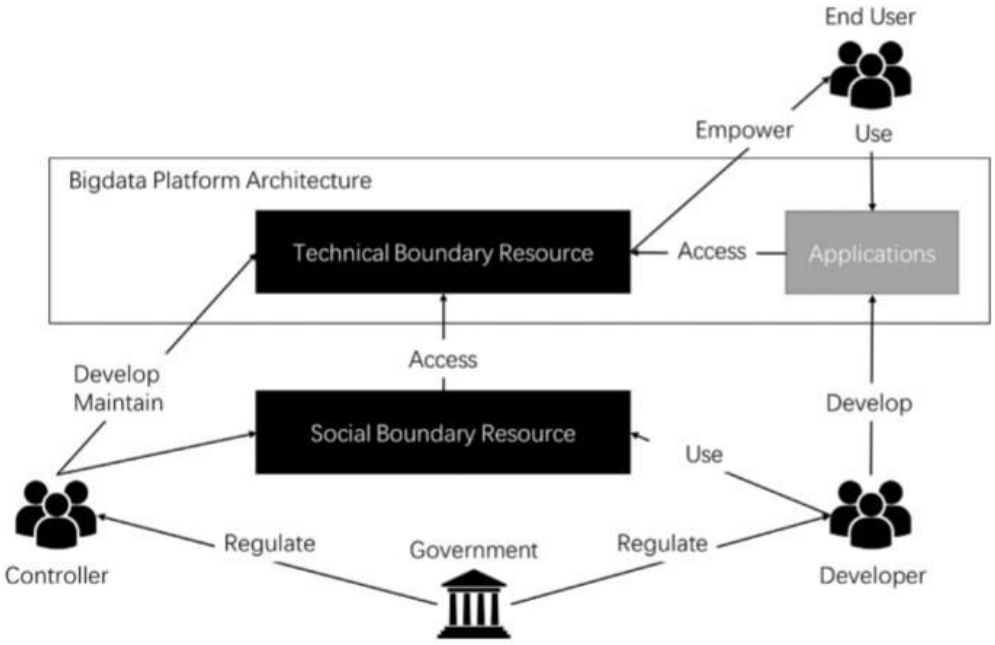

Fig. 2. Boundary resource perspective.

IMPORTANCE OF DIGITAL PRIVACY IS MONUMENTAL

Without digital privacy your data can be harvested and potentially……

• Data about your calculated health and health risks can be sold to insurance companies, who can either deny you as a client or decrease/increase your subscription fee.

• Data about your predicted voting patterns can be sold, and if you are

• Calculated data about your cognitive abilities, lifestyle and psychological makeup

What does privacy mean in the digital age?

In the virtual world where every action we take can be tracked, however, privacy may seem more like an ideal concept than a reality. Your search history, the posts you 'like' on social media, and every keystroke you make on a digital device-you may expect this

information to be private, but too often it is not.

ONLINE PRIVACY CONSTRUCTS

In this chapter the factors that influence customers' online privacy perceptive discussed. Based on former research of privacy in the online and offline environment 4/15 measurement and connection between privacy concerns and customer behaviour, a. factors were identified that have influence on customer's privacy concerns. The Research described in this article will predominantly focus on e-commerce privacy issues. In order to include factors from all aspects of privacy a factor categorization is proposed. It is based on the following groups which organize the various factors that influence the Internet users privacy concerns:

1. Customer-intrinsic factors:
2. Customer perceptions, beliefs and attitudes toward direct marketing and/or in-home shopping, trust, mechanisms for information control, and processes of data collection;
3. Web site related factors: 4. Situational factors: According to some authors, besides the four groups of factors proposed above, one or more other groups (of factors) can be conceptualized that are related to legislation and Government protection

RESEARCH MODEL ON ONLINE PRIVACY

According to the Internet World Statistics, 23.8% of the world's population today uses the Internet. The widespread use of the World Wide Web as well as the customers' positive response to this kind of technology has opened the way to many types of business, among which online shopping and e-banking are the most widely used. However, there is no detailed information about the factors that influence online shopping or e-banking acceptance,

About the factors that influence customer behaviour when using these e-services. Therefore a research model of online privacy perceptions of e-banking/online shopping users is proposed. The proposed research model is illustrated in the figure. It proposes a relationship between Internet users'

privacy perception and (1) customer-intrinsic factors, (2) customer and web site relationship. (3) web site characteristics, (4) situational factors and (5) legislation and government protection group of factors. For each group there are also illustrated constructs (scales) that are measured. By following the proposed categorization of factors that have influence over consumer's online privacy concerns, and an examination of the existing privacy literature a set of 94 items was collated. Items were created in three ways: (1) by using original items from previous work, (2) through modification of the original items, and (3) by creating new items.

Users' perception of the level of privacy protection when using e-banking/online shopping services was measured using a four-item scale. Scale was named User's privacy perception. User's privacy perception refers to user's evaluation and anxiety about how an online company or a bank will handle information that they collect about the users. Also, users' satisfaction with privacy protection during their online activity (everyday online activity), as well as satisfaction with privacy protection when using e-banking or online shopping services were measured (by using one item scale for each). Users' satisfaction with privacy protection during their online activity (everyday online activity) refers to the users' satisfaction with privacy practices (protection mechanisms) that an online service provider uses to secure users' online privacy. Users' satisfaction with privacy protection when using e- banking or online shopping service refers to the users' satisfaction with the ways in which an a bank or online company secure and protect users' online privacy. Items were based on the five-point Like scale

relationship. Companies use all possible

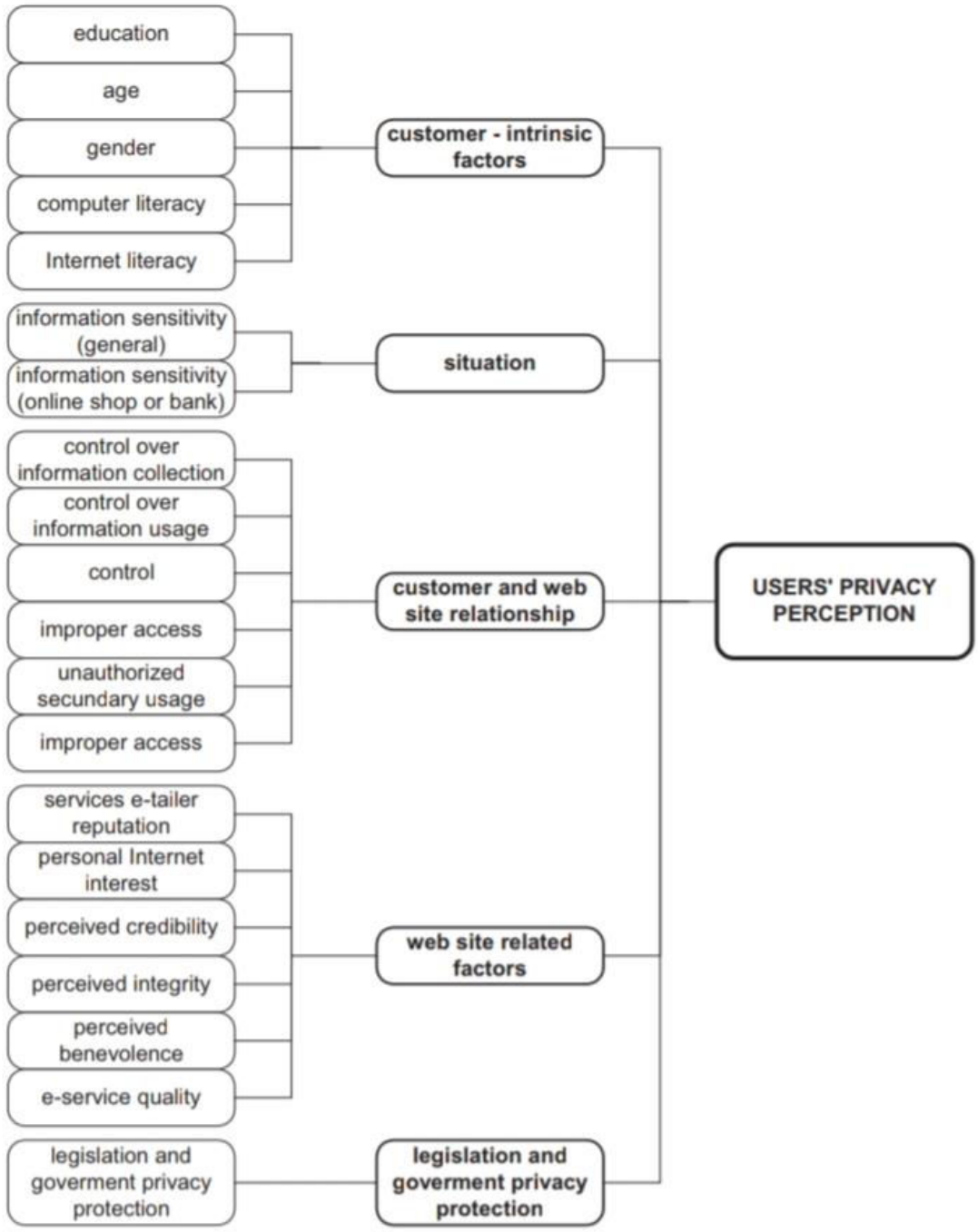

Figure . Research model of e-banking/online shopping users' privacy perception

CONCLUSION

Information is a significant resource in the present customer-supplier ways to collect information about their customers in order to offer services or products that better meet their customers' needs and desires. Although new technologies offer increased

capabilities of collection, storage, usage and dissemination of information, collecting and using customer information in a way that would make customers feel comfortable presents a challenge for companies. The information that is being collected in online transactions is not only related to the personal information of specific customers but also to information about their preferences in shopping, hobbies, and lifestyle. When customers become aware of all the possible consequences of information collection (and usage) about them, their privacy concern is likely to be raised.

Every day people can read in the newspapers or on Internet portals (or hear on TV) about new cases of data loss, situations where data were stolen or data were sold to the third party. People are becoming nervous and very careful about their personal information. Privacy and fraud are viewed as main causes of the limited usage and expansion of e-commerce. Privacy in online environment covers issues related to user's concerns for his personal information collection, storage, usage and dissemination. Fraud is one of possible consequences of improper handling of user's personal information and (some) companies aim to maximise their profit. Internet user's privacy concerns can be viewed through:

(1) concern for personal information collection by a third party;

(2) concernrelated to collected personal information storage/archiving:

(3) concern for collected personal information collation and dissemination;

(4) concern for DE contextvalidation of the Internet user's personal information.

Results of the research presented in this article confirm this. According to the results users online privacy perception is influenced by

(1) user's perception of control over information collection during their everyday online activity,

(2) type of information that are asked in order to perform a transaction,

(3) concerns regarding improper access to information that were collected,

(4) user's perception of information collection during their interaction with a bank or an online company through a web site,

(5) user's perception of Internet privacy risk,

(6) and perception of legislation and government privacy protection.

Online privacy protection should be the responsibility of all participants that are included in the online market. First of all, an individual must take responsibility for his information. He should value and protect his personal information. He must understand and make decisions about what information he should and shouldn't share. In addition, when entering an online transaction he must understand how and which information (about him) will be collected. An individual must obtain knowledge about the length of time the collected information will be kept, who will have access to them, for which purpose they will be used, and how will they be secured. Internet user should not be a passive participant in an online transaction, and shouldn't allow an online company to force him to share his personal information. User should actively protect his information (use all possible protection mechanisms) and ask/demand of the online company (or any organization that is participating in online market) to protect his online privacy,

Furthermore, online companies (organizations that offer their services or products online) should take responsibility for protecting and securing customers' online privacy. They should recognize that the customer's perceptions of privacy protection in actual interactions are of significant importance to customers when they decide to conduct business with a specific company in the future. Therefore, they should inform customers about privacy practices that they use. Online companies should define their responsibilities and behaviour regarding protection of customer personal information. They should use all possible mechanisms to make clear to their customers that they will not misuse the collected information or sell it (like using a privacy seal, privacy policy). When developing a new information system an online company should pay attention to implement all customers' needs regarding protection of his personal information. Furthermore, study results that were presented could be used to improve new e-service development or a modification of present e-services. At the very beginning. When defining an

e-service, online company should include these requirements (customers requirements regarding their online privacy protection). First, the new e-service should include mechanisms that will give the customer control over his information collection. Online company should the ask customer's permission to collect information about him, and his activity on a specific (online company's) web site. Second, online company should protect the collected customer information from improper access. There are many new technology-based solutions regarding these issues. Online company should revise all possible solutions and incorporate them in access control. Accordingly, the customer should be informed. Finally, online company should regulate customer online privacy protection according toPresent privacy legislature.

REFERENCE

- Ashwort, L; Free, C, Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns. Journal of Business Ethics, 67:107-123, 2006…
- Bauer, H.H. Hammerschmidt, M. Falk, T. Measuring the quality of e-banking portals.International Journal of Bank Marketing, 23(2): 153-175, 2005 Berendt, B. Teltzrow. M. Addressing user's privacy concerns for improving personalization quality towards an integration of user studies and algorithm evaluation. In Intelligent Techniques for Web Personalization, LICAL 2003 Workshop, ITWP 2003.Pages 69-88, Acapulco, Mexico, 2003.
- Burgoon, J. Privacy and communication. In Communication Yearbook 6, pages 206- 249, Beverly Hills, California, 1982.
- Buchanan, T. Paine, C; Joinson, A.N: Reips, U-D. Development of measures of onlineprivacyconcem and protection for use on the internet. Journal of the American Society for Information Science and Technology, 58(2):157-165, 2007. 6. Castañeda, J.A; Montoro, F.J. The effect of Internet general privacy concern oncustomerbehavior. Electronic CommerceRewarch, 7(2):117-141, 2007.

- Castañeda, JA; Montoso, FJ; Luque, T. The dimensionality of customer privacy concern on the intemet. Online Information Review, 31(4): 420-439, 2007.
- Chellappa, R.K. Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. www.bus.emory.edu/ram/Papers/sec-priv.pdf.downloaded: December, 22" 2009.
- Dinev, T. Hart, P. An extended privacy calculus model for e-commerce transaction. Information System Research, 17(1):60-81, 2006.
- Dolnicar, S; Jordan, Y. Protecting customer privacy in comparty best interest.Australasian Marketing Journal, 14(1):39-61, 2006, 11. Eastlick, M.A; Lotz, S.L; Warrington, P. Understanding online B-to-C relationships: anintegrated model of privacy concerns, trust, and commitment. Journal of BusinessResearch, 59(8):877-886, 2006,
- Goldie, J. Virtual communities and the social dimension of privacy. University of Ottawa Law and Technology Journal, 3(1):133-167, 2006.
- Harkiolakis, N. A six-dimensional approach to online privacy, IBLT 2006-Copenhagen. http://harkiolakis.org/research/Privacy/A Six-Dimensional Approach to Privacy.ppt, downloaded: December, 22 2009.
- Internet World Stats, usage and population statistics, Internet usage statistics,http://www.internetworldstats.com/stats.htm, downloaded: December, 22" 2009,
- Jih, W-J; Wong, S-Y; Chang, T-B. Effects of perceived risks on adoption of Internetbanking services: an empirical investigation in Taiwan International Journal ofBusiness Research, 1(1):70-88, 2005.