Volume 11, July 2020 ISSN 2581-5504

"Privacy and Security Issues in E-Commerce"

*Antra Pandit
Rajiv Gandhi National University of Law, Punjab

ABSTRACT

This paper will mainly concern with e-commerce and its significance in present scenario and will majorly focus on how the privacy of an individual is compromised in this electronic marketing environment. Also the study will deal with the security challenges faced in the processes of online businesses. The present paper would primarily talk about the present legal measures in different countries to regulate the e-commerce. The study would highlight the legal framework pertaining to e-commerce in India and also drive attention to the major drawbacks with law for e-commerce prevailing in India and what measures can be taken to fill the gap of regulation.

INTRODUCTION

Commerce is the continuance of business using the Internet with the help of web. E-commerce business becomes very popular now-adays and comes into light with many privacy issues. As the result, users leave this platform, if these issues are not combatted, users will refuse to do online transactions.[1] Privacy and security are emerging issues in e-Commerce. One of the concerns of e-commerce is the need to maintain users' privacy online. Consumers are concerned about the unauthorized access to their data and the growth of e-Commerce depends on the security and privacy policies put in place to gain the trust of consumers. E-Commerce sites are an obvious target and many of them are not sufficiently safeguarded against the threat of cyber-attacks.[2] The usage of technical means to track down user's surfing and purchasing tendencies by the use of cookies, and sniffers to capture data while in the course of transmissions, has raised significant privacy issues.[3] Doing some electronic business on the Internet is already an easy task as well as cheating and snooping is also easy. There are several reasons that contribute to this insecurity such as; The Internet does not offer much security. Eavesdropping and acting under false identity is simple. Stealing data is undetectable in most cases. Popular PC operating systems offer little or no security against virus or other malicious software, which means that users cannot even trust the information displayed on their own screens. At the same time, user awareness for security risks is threateningly low.[4] Privacy issue is gaining more and more attention, as in present times our lives are being exposed to the media through social networking sites to a greater extent, what

*LL.M, Rajiv Gandhi National University of Law, Punjab

[1] Budak C, Goel S, Rao J, Zervas G (2016) Understanding emerging threats to online advertising. ACM Conference on Economics and Computation pp: 561-578

[2] https://www.jeffbullas.com/data-privacy-and-security/

[3] https://www.tandfonline.com/doi/abs/10.1080/13600602760586769

[4] https://www.uniassignment.com/essay-samples/information-technology/privacy-and-security-issues-in-ecommerce-information-technology-essay.php

to share that too how much to share has become the point to think for. The security challenged faced on online platform is transversal; it has undisputed cross-border nature. There is high vulnerability of attacks to the websites offering services on internet which could result in blockage of sites, denial of service. The actions like this could result in crisis situation due to an unauthorised use, leading to compromise of data and financial loss, sometimes the infrastructure such as power grids, LAN networks, internal security system of any organisation etc. could become targets causing financial loss, loss of human resources and can lesser the confidence of public at large. Cybercriminals are using various techniques to access the database of your e-Commerce store where you store valuable customer information. The European Union enacted the GDPR partially in response to these concerns. Closer to home, California passed the California Consumer Privacy Act ("CCPA").

IMPACT ON & OF E-COMMERCE

E-business owners are exploiting the user's privacy for the growth of their business. Different authors have the different meaning of privacy as Etzioni belief that societally illegitimate and infeasible measure is defined as privacy.[5] According to Davies, it's a squandered right.[6] Experience shows that the users are concerned about the unauthorized access to their data. They never permit to reuse their personal data or sell it for the business purposes. Now-a-days online providers are specific on their privacy strategy.[7]

The growth and trust upon E-Commerce business totally depend on the security and privacy policy of the site and for the development of E-commerce business most important factor is to build trust among users.[8] To maintain privacy in the E-commerce business, a complete and secure system is required.[9] Users feel hesitation in E-Commerce although online payment system is more secured and convenient.[10]

E-Commerce is going to evolve continuously, as for instance it was witnessed that there was total 135% of increase in sale from 2009 to 2015[11]. Due to M-Commerce i.e. Mobile

[5] Lee I (2016) User Privacy Concerns for E-Commerce. IGI Global:Encyclopedia of E-Commerce Development, Implementation, and Management pp: 1780-1787

[6] Ackerman MS (2004) Privacy in pervasive environments: next generation labeling protocols. Personal and Ubiquitous Computing , 430-439

[7] Ackerman MS, Davis TD (2003) Privacy and security issues in e-commerce. New economy handbook pp: 911-930

[8] Smith R, Shao J (2007) Privacy and e-commerce: a consumer-centric perspective. Electronic Commerce Research 7: 89-116.; Corbitt BJ, Thanasankit T, Yi H (2003) Trust and e-commerce: a study of consumer perceptions. Electronic commerce research and applications, 203-215

[9] Lau RY (2007) Towards a web services and intelligent agents-based negotiation system for B2B eCommerce. Electronic Commerce Research and Applications, 260-273

[10] Castañeda JA, Montoso FJ, Luque T (2007) The dimensionality of customer privacy concern on the internet. Online Information Review, 420-439

[11] The Evolution of Ecommerce; *available at*, https://www.webfx.com/blog/general/the-evolution-of-ecommerce/, last accessed on 15-11-2019.

Volume 11, July 2020 ISSN 2581-5504

Commerce the e-commerce is reaching to the level next, in coming years it is expected to be at its zenith.

Advantages of e-commerce

With the introduction of e-commerce huge changes are being witnessed in almost every field. It has reduced the distance of globe, by making one common market for all. It has impacted life of a common man to large extent, likely to be the best ever thing happened to the people. Now it is easier to buy or sell products, services or information at anytime anywhere. Following are the advantages of e-commerce:

I. Availability 24*7: e-commerce is omnipresent. With the introduction of mobile phones for that mobile commerce too, the market is just a click away. One can shop; make deals at any time at any places unlike the traditional markets which are time bounded a place restricted.
II. Accessibility: it makes service easily accessible to all, look for product, get thousands of options choose whatever you want too without any urgency or disturbance according to your wish. No need to be the part of crowd, that too for limited options.
III. No geographical barriers: e-commerce has overcome the geographical barrier. One can place order of any product from any country by any sitting in his home thousands kms away.
IV. Cost effective: due to advancement of technology and of online marketing the cost of the products and services has reduced. Even high market competition is our reason for it the call to survive in market. Less physical labour and presence required has made it most cost effective.

Disadvantage of e-commerce

Nothing comes only with advantages everything has its own cons or disadvantages too. Same is with e-commerce too; following are the disadvantages of e-commerce:

I. Security issues: this is the first and foremost issue faced which being on online virtual platform. The risk of hacker is there, one save their payment cards detail on a particular site, though sites carry all measures to secure it but there is constant threat that it may be hacked and all your provided details may be misused.
II. Unemployment: due to maximum dependence on electronic ways or handlers the physical presence of man is less required. Also the traditional markets are getting impacted due to which more unemployment is generated, as people are having less technical skills to find some other way-out.
III. Lack of privacy: most of the websites do not have high encryption to protect the online details provided by the customer like account details, digital signatures, documents etc. and wrongdoers are always in search of loopholes. They take this

information and use them for their own profits and your loss i.e. to achieve their bad intentions.

IV. Legal issues: in some developing countries there are no strong laws that can deal with the cyber crimes, laws are not much clear that are governing the e-commerce transactions.

V. No physical presence: like in traditional market if one has some query or issue related to some product or services one can ask and can clear doubts and be satisfied, but here there is no such thing mostly it's all computerised automated, most of the time keeping customers on hold, if they call for issues.

There are four categories of antecedents that influence consumer trust and consumers' perceived risk towards electronic commerce entities[12] which are:

1. *Experience-based*: e.g., e-commerce experience, familiarity, Internet experience, etc.
2. *Cognition (observation)-based*: e.g., system reliability, privacy protection, quality of information, security protection, brand image, etc.[13]
3. *Personality-oriented*: e.g., disposition to shopping habbits, trust, etc.
4. *Affect-based*: e.g., presence of third-party seals, reputation referral, recommendation, buyers‟ word-of-mouth, feedback, review comments, etc.[14] Ecommerce web site owners on one side are thinking of how to attract more customers and how to make the visitors feel secured when working on the site, while on the other side how the end users should rate a ecommerce website and what they should do to protect themselves as one among the online community.[15] Each phase of E-commerce transaction has security measures.

Technologies used for E-Commerce Privacy

Majorly there are four broad categories of privacy technologies

1. technologies used for surveillance
2. technologies for forming contracts or agreements about the release of private data
3. technologies for labeling and trust, and
4. privacy-enhancing technologies (PETs). The technologies for surveillance and for data capture are used by companies for business purposes, but they have the side effect of generating biometrics, data trails, data warehousing and data mining thus affecting personal privacy. However, privacy enhancing technologies (PETs) attempt to balance the surveillance

[12] J.B. Barney, M.H. Hansen. Trustworthiness as a source of competitive advantage. Strategic Management Journal, 15 (1994), pp. 175–190

[13] C.C. Chen, X.-P. Chen, J.R. Meindl. How can cooperation be fostered? The cultural effects of individualism–collectivism. Academy of Management Review, 23 (2) (1998), pp. 285–304

[14] D .J. McAllister. Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. Academy of Management Journal, 38 (1) (1995), pp. 24–59

[15] V.Srikanth "Ecommerce online security and trust marks". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July-September (2012).

Volume 11, July 2020 ISSN 2581-5504

or tracking technologies through personal firewalls, cookie managers and digital cash (e.g., Ecash).[16]

ROLE OF EDI

With the coming of EDI Electronic Data Interchange the milestone to the beginning of new era was set up. EDI can be used to exchange business documents such as purchase order, invoices, and payments through electronic medium among the trading partners. EDI is not same as emails, or sharing data through networks. It is a kind of platform where both sender and buyer uses same agreed format, processes through which documents can be exchanged. The standard of exchanging data is always in pre defined format, EDI translates any common file into the format of pre defined one. The basic computerisation is required to get all advantages of EDI. Due to implementation of EDI the most of the data sharing process has gone automated which has further reduced the operational costs, delays in deliver and human or administrative error. Due to this now there is quick transfer of documents with decreased errors, resulting efficiency in services, the orders are met on time and sometimes even before time. The management of information is easy and efficient. The relations with customers are getting stronger, through better quality services.

To send and receive data or messages through EDI three basic components are required:
EDI Standards; these are the standards which includes syntax and semantics of the data which has to be exchanged. These standards set a particular pattern or format in which data is to be accepted. ANSI X12 Standards were developed by ANSI[17] for the use of all US businesses, later it was followed by UN/EDIFACT (EDI for Administration, Commerce and Transport) Standards announced by UN in 1987 for international trade[18].
EDI Software; it is a software that translates unorganised, company specific format to structured EDI format and also converts EDI format to company specific format. Before coming of UN/EDIFACT there were multiple standards which were being followed. So it's important for good EDI software to be able to handle multiple standards.

Communication networks; the communication networks like internet and extranet are used as EDI medium to exchange documents electronically. The data exchanged is stored on the server so that it can be downloaded and uploaded at convenience. These networks act as a single interface for users rather than handling multiple one.

[16] Palak Gupta, Akshat Dubey; E-Commerce- Study of Privacy, Trust and Security from Consumer's Perspective; IJCSMC, Vol. 5, Issue. 6, June 2016, pg.224 – 232
[17] American National Standards Institution
[18] K.Bajaj and D.Nag, E-Commerce; the Cutting Edge of Business, Second Edition, Tata McGraw Hill, New Delhi, 2011.

Volume 11, July 2020 ISSN 2581-5504

PRIVACY IN E-COMMERCE

Privacy is a serious issue in electronic commerce, no matter what source one examines. Culnan[19] argued that privacy concerns were a critical reason why people do not go online and provide false information online. Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses.[20] The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce. Some people consider privacy to be a fundamental right; others consider it to be a tradable commodity. Besides "privacy", a number of terms such as, digital persona, notice, identification, choice, authentication, pseudonymity, anonymity, and trust are also major concerns in e-commerce to be addressed. E-commerce sites could potentially collect an immense amount of data about personal preferences, shopping patterns, patterns of information search and use, and the like about consumers, especially if aggregated across sites. Not only it is easier than ever to collect the data, but also much easier to search these data.[21] New computational techniques allow data mining to explore consumer"s buying patterns and other personal trends in almost real time mode. Consumers have two kinds of privacy concerns. First, they are concerned about the risk of secondary use i.e., the reuse of their personal data for unrelated purposes without their consent such as sharing with third parties who were not part of the transaction in which the consumer related his or her personal data. Second, consumers are concerned over unauthorized access to personal data because of security breaches or the lack of internal controls[22]. As we are witnessing that e-commerce is leading us to a shift to digital world. Initially only buying and selling was the part of e-commerce but now the scenario is not same, it has now included almost every sphere of activity. Name a thing or service which is not available to us on the click of a button. But as it has been witnessed that technology is both boon and bane for the evolving society. It has made our life easier, more convenient and faster but at the same time there is a continuous threat, sense of insecurity of being victim of cyber crimes. Cyber crimes are very real, as they can cause huge financial loss to society and can they harass the citizens in different ways. These crimes can be in any form, from violating privacy of an individual to threatening the security of a nation.

Privacy issue is gaining more and more attention, as in present times our lives are being exposed to the media through social networking sites to a greater extent, what to share that too how much to share has became the point to think for. Many company's websites tends to

[19] Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10 (1) : 104-115.
[20] Dhillon, Gurpreet S., and Trevort T. Moores. 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4) : 33-37
[21] Winner, D. 2002. Making Your Network Safe for Databases. SANS Information Security Reading Room, July 21, 2002
[22] Dhillon, Gurpreet S., and Trevort T. Moores. 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4) : 33-37

create users profile to track their choices, interests, for which they ask for data. The amount of data taken by them, they do not realise that this much information is required or not or even is it relevant. The security challenged faced on online platform is transversal; it has undisputed cross-border nature. As systems are connected to internet they are at high potential to get targeted and could result in tampering of data store in them. There is high vulnerability of attacks to the websites offering services on internet which could result in blockage of sites, denial of service. Any unauthorised person pretending to be the authorised one could attain access to one's system and can and modify or alter changes to gain profits or personal interests. The actions like this could result in crisis situation due to an unauthorised use, leading to compromise of data and financial loss. With the growing Trend of e-commerce such incidents create distrust in the networking and online system. Systems, networks have to be protected otherwise the infrastructure such as power grids, LAN networks, internal security system of any organisation etc. could become targets causing financial loss, loss of human resources and can lesser the confidence of public at large.

CHALLENGES IN E-COMMERCE IN SPHERE OF PRIVACY

Cyber crimes can be in any form, from violating privacy of an individual to threatening the security of a nation. There are almost 21% of the crimes related to privacy and security. The numbers of cases registered under the IT Act and IPC have been growing continuously. The cases registered under the IT act grew by more than 350% from 2011 to 2015; there was almost a 70% increase in the number of cyber crimes under the IT act between 2013 and 2014, there are more number of cases registered under IT Act then IPC.[23] Some of the acts that impacts on the privacy and the security of an individual or organisations that are the part of e-commerce or online activities are as below:

Program based attacks: in this type of attack a program is made and executed on the targeted system by following ways;

I. **Trojan**- though this program appears to be useful but has potential to function malicious that is it can evade security mechanism by exploiting legitimate authorisation of system. The modified version to do nasty things like gaining access to sensitive data, spying, to exploit someone etc is known as Trojan horse attack. It is a Malware and cannot act as self replicator.

II. **Virus**- it is self replicating computer software with malicious logic that propagates by using any infected copy, opening any unauthorised site that is infected, accepting any unauthorised email, clicking on an executable file, using infected storage devices.

III. **Worms**- it is a computer program that can run independently or we can say it is a standalone Malware that replicates itself on its own In order to spread to further system. It causes harm to network by affecting its bandwidth or it also consumes space in system

[23] https://factly.in/cyber-crimes-in-india-which-state-topsthe-chart/, last accessed on 19-11-2019.

Volume 11, July 2020 ISSN 2581-5504

IV. **Spam**- there were an estimate according to which 70% of all email is actually spammed that is junk mail. The spam appears to be as a promotional material or an advertisement email, of which user unexpectedly becomes victim. This kind of program is used to collect information or data related to the interest or activities of concerned user by way of spam one can even spy on the target[24]. This is one form of information espionage, used by market competitors with the purpose to steal the market of targeted one.

E- COMMERCE SECURITY ISSUES

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with any resulting bad publicity and break-ins. There are a number of critical social and organizational issues with security. The first is the development of adequate organizational processes for risk management, development of security policies, separation of duties, security assurance and access control. The second is that the weak link in security is often employees or users, rather than the technology[25] and the third is software engineering management, or managing how security technology is deployed.

TECHNOLOGIES USED FOR E-COMMERCE SECURITY

1. Encryption algorithms like Public Key Infrastructure (PKI) systems which are based on asymmetric cryptography are highly secure as they are coupled with Secure Socket Layer (SSL) protocol and the interbank standard suite, ANSI X9. PKI often requires a centralized, highly available intermediary for key management, and especially for prompt notification about revoked key-pairs.[26]
2. A digital signature, which can be used to sign contracts, to prove identity for access or to provide authenticity of an electronic distribution is the best example of PKI.
3. Smartcards[27] can be used to store data about the bearer of the card, including identification credentials, financial data, medical records etc. Smartcards can allow POS transactions to be more intricate, because the entire user's data is always available. This architecture can also avoid the centralized storage of personally sensitive data.
4. Digital cash and networked payments through which a consumer might buy electronic data or a digital service without revealing his purchases to a financial clearinghouse and identity to the merchant.[28] Micropayments such as per-article newspaper subscriptions and PayPal, a payment intermediary, have also been financially successful.

[24] K.Bajaj and D.Nag, E-Commerce; the Cutting Edge of Business, Second Edition, Tata McGraw Hill, New Delhi, 2011, p. 252.
[25] Schurr, P.H. and Ozanne, J.L. (1985), ``Influences on exchange processes: buyers‟ preconceptions of a seller‟s trustworthiness and bargaining toughness‟‟‟, Journal of Consumer Research, Vol. 11 No. 4, pp. 939-53
[26] Rankl, W., and W. Effing. 1997. *The Smartcard Handbook*. New York: John Wiley
[27] Chaum, David. 1985. Security Without Identification: Transaction Systems To Make Big Brother Obsolete. Communications of the ACM, 28 : 1030-1044.
[28] Delaigle, J-F., C. De Vleeschouwer, and B. Macq. 1996. Digital Watermarking. Proceedings of the Conference 2659 - Optical Security and Counterfeit Deterrence Techniques : 99-110.

5. Digital watermarking technology[29] is another popular internet security mechanism where the technical goal is to find ways of cryptographically tagging electronic content (especially images and audio) in a way that is non-removable, non-forgeable, and recognizable. The watermark tag is generally designed to be invisible or unobtrusive.

INTERNATIONAL LEGAL FRAMEWORK ON PRIVACY IN ONLINE BUSINESS

The remarkable development in the e-commerce sector has also led to many problems relating to the protection of rights of consumers on online platform. The main concern of every country regarding e-commerce are as security of payment, data protection, validity of e-contracts and likewise. To deal with these kinds of challenges different countries have formulated different legislations. Some of the legislative measures by different countries are as below:

I. **MALAYSIA:** The Malaysia Consumer Protection Act 1999 (CPA), initially does not includes e-transactions, but later in 2007 amendment, the provision was added as 'any trade transactions conducted through electronic means'. The aim of this amendment was to protect the rights of e-consumers. There were further amendments in 2010 to CPA, in which provisions were added for protection of e-consumers against misleading and deceptive conduct, also for unfair trade practices[30]. With these many amendments it is now obligatory to online traders to provide the consumers with sufficient and correct information about the concerned product.

II. **EUROPEAN UNION:** Article 16 protects the confidentiality of personal data, by prohibiting any person who has access to personal data to process them ―except on instructions from the controller, unless he is required to do so by law. Article 17 of Directive 95/46/EC mandates the undertaking of ―appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing[31]. Data protection is a fundamental right enshrined in Article 8 of the EU Charter of Fundamental Rights, which is distinct from respect for private and family life contained in Article 7 of the Charter. UK though it's not the member state of EU any more, still it is following the Data Protection Act 2018, which significantly focuses on data subject rights, "special category" personal data,

[29] Anderson, Ross. 1994. Why Cryptosystems Fail. *Communications of the ACM*, 37 (11) : 32-40.

[30] Legal Framework for E-commerce Transactions and Consumer Protection: A Comparative Study; Muhammad Nuruddeen, Nor Anita Abdullah, Yuhanif Yusof, 2016; *available at*, https://www.researchgate.net/publication/315730418_Legal_Framework_for_E-commerce_Transactions_and_Consumer_Protection_A_Comparative_Study, last accessed on 19-11-2019.

[31] Maria Grazia Porcedda, "Data Protection And The Prevention Of Cybercrime: The Eu As An Area Of Security?", *EUI Working Papers*, European University Institute, Department of law, p. 12.

data protection fees, data protection offenses, consent from children and enforcement, transfer of data to other country[32].

III. **GERMANY:** the country has been and continues to be a leader in privacy protection with robust laws that provide more protection than many other jurisdictions. "The country's Federal Data Protection Act 2017 (Bundesdatenschutzgesetz – BDSG), works alongside the GDPR[33] (2016/679) to outline the general obligations of personal data collectors and processors. The provisions in the BDSG apply to public and private bodies that collect or process personal information with several exceptions. Main provisions in the BDSG include the designation of a DPO, rules for scoring and credit checks, criminal law provisions and rules for employment-related data processing"[34]. Also contains provisions related to subject's rights, informed consent etc.

IV. **USA:** there is no comprehensive law in USA to govern data protection or online activities. In fact it has sector specific laws and state laws to deal with the issues of e-commerce. There are more than 15 laws at sector specific level and more than 100 laws at state level for privacy. It relies on a "combination of legislation, regulation and self-regulation" rather than government intervention alone. The most prominent national laws include the Privacy Act 1974, the Privacy Protection Act 1980, the Health Insurance Portability and Accountability Act 1996, the Fair Credit Reporting Act 2018. The Privacy Act "prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements."[35]

V. **AUSTRALIA:** Federal Privacy Act 1988 is the key privacy law that governs both the public and private sectors. The Privacy Act is based on 13 Australian Privacy Principles (APPs) that cover transparency and anonymity; the collection, use and disclosure of data; security of information; access to personal information; maintaining the quality of data; and the data subject's rights[36]. In addition to this data protection is governed by statutory privacy laws applicable in the majority of Australian states and sector-specific privacy law. For example, organizations that collect, use or disclose health data are governed by separate Health Privacy Principles[37]. Organizations in Queensland that deal with personal data will also be governed by the Information Privacy Act 2009.

[32] Data Protection Act 2018; *at*, http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted, last accessed on 20-11-2019.
[33] EU General Data Protection Regulation
[34] https://www.bfdi.bund.de/DE/Home/home_node.html, last accessed on 21-11-2019.
[35] Privacy Act Of 1974; *at*, https://www.justice.gov/opcl/privacy-act-1974, last accessed on 21-11-2019.
[36] Australian Privacy Principles; *at*, https://www.oaic.gov.au/privacy/australian-privacy-principles, last accessed on 20-11-2019.
[37] A Practical Guide to Data Privacy Laws by Country, Katie Yahnke; 2018; available at, https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/, last accessed on 20-11-2019.

VI. **CANADA:** At the national level, the collection, use and disclosure of personal information in the private sector is governed by Bill C-6 of the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. PIPEDA was most recently amended in November 2018 to include mandatory data breach notification and record-keeping laws[38]. For the public sector, such as federal departments and Crown Corps., data privacy is governed by the Privacy Act 1983. Canada has 28 federal each having its own statutes to govern data privacy policy.

INTERNATIONAL BODIES ON E-COMMERCE

A. United Nations Commission on International Trade Law (UNCITRAL)

UNCITRAL formed model laws with an intention that developing countries would adopt these laws in interest of harmonizing national law in order to promote economic development. Following are the UNCITRAL Model laws:

I. **UNCITRAL Model Law on Electronic Transferable Records[39] (2017):** It aims to enable the legal use of electronic transferable records both domestically and across borders. The MLETR applies to electronic transferable records that are functionally equivalent to transferable documents or instruments. Transferable documents or instruments are paper-based documents or instruments that entitle the holder to claim the performance of the obligation indicated therein and that allow the transfer of the claim to that performance by transferring possession of the document or instrument.

II. **UNCITRAL Model Law on Electronic Signatures[40] (2001):** aims to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. Thus, the MLES may assist States in establishing a modern, harmonized and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status.

III. **UNCITRAL Model Law on Electronic Commerce[41] (1996):** it is intended to overcome obstacles arising from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for enabling the use of paperless communication, thus fostering efficiency in international trade.

[38] The Personal Information Protection and Electronic Documents Act (PIPEDA); *at*, https://www.priv.gc.ca/en/, last accessed at 20-11-2019.

[39] UNCITRAL Model Law on Electronic Transferable Records 2017; *at*, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records, last accessed on 15-11-2019.

[40] UNCITRAL Model Law on Electronic Signatures 2001; *at*, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records, last accessed on 15-11-2019.

[41] UNCITRAL Model Law on Electronic Commerce 1996; *at*, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records, last accessed on 15-11-2019.

Volume 11, July 2020 ISSN 2581-5504

B. Organization for Economic Cooperation and Development (OECD)

E-commerce has evolved dramatically since 1999, when the OECD Council adopted the first international instrument for Consumer Protection in the context of Electronic Commerce ("1999 Recommendation"), on 24 March 2016, the OECD Council revised this instrument and the Recommendation of the Council on Consumer Protection in E-commerce ("the revised Recommendation") now addresses new and emerging trends and challenges faced by consumers in today's dynamic e-commerce marketplace[42]. It laid down certain recommendations which focus on bringing more transparency and protection in e-commerce. It recommended that government and stakeholders should work together to achieve the concern goal. It talked about dealing with security and privacy issues by recommending businesses to provide all reasonable security safeguards to ensure security of the data provided by the customers, to manage the digital security risk; to reduce adverse effect on customer's involvement in e-commerce.

C. World Intellectual Property Organization[43]

WIPO has created a Digital Agenda to respond to the confluence of the Internet, digital technologies and the intellectual property system. Through international discussions and negotiations, WIPO is formulating new ways in which intellectual works can be disseminated, while at the same time ensuring the rights of their creators remain protected.

D. World Trade Organization[44]

At the Second Ministerial Conference in May 1998, ministers, recognizing that global electronic commerce was growing and creating new opportunities for trade, adopted the Declaration on Global Electronic Commerce. The Declaration instructed the General Council to establish a comprehensive work programme to examine all trade-related issues relating to global electronic commerce, including issues identified by Members. The Council for Trade in Services to examine and report on the treatment of electronic commerce in the GATS legal framework; the intellectual property issues arising in connection with electronic commerce; on the development implications of electronic commerce. The General Council's examination of cross-cutting issues under the Work Programme has been carried out in dedicated discussions held for this purpose. The twelfth and most recent Dedicated Discussion was held on 18 October 2016. Since then, discussions have continued in informal open-ended meetings convened by the General Council Chair and through the review of progress in the General Council.

[42] Consumer Protection in E-commerce: OECD Recommendation, Consumer OECD (2016); *at*, https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf, last accessed at 15-11-2019.
[43] http://www.wipo.org., last accessed on 21-11-2019.
[44] Electronic commerce; at, https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm, last accessed on 21-11-2019.

Volume 11, July 2020 ISSN 2581-5504

Due to the privacy trust issues, The Organisation for Economic Co-operation and Development (OECD), the U.S. government and the European Union began extensive discussions about developing a regulatory framework for privacy. These discussions were guided by eight privacy principles

i. Collection Limitation
ii. Data Quality
iii. Purpose Specification
iv. Use Limitation
v. Security Safeguards
vi. Openness
vii. Individual Participation
viii. Accountability

The European Union in 1995 decided to adopt formal enforcement in the form of the Data Protection Act[45] incorporating the eight OECD principles, while the United States, although endorsing the principles, adopted the self-regulation approach rather than governmental regulation.[46]

DIFFERENT DATA PROTECTION APPROACHES

i. Self-Regulation approach

In the self-regulation approach, data protection in an e commerce context is left mostly to the evolution of industry norms and voluntary compliance. This approach is being used in the United States. Each company is responsible for deciding on the degree of information that is collected and used, and for developing its own privacy policy statement based on its industry guidelines.[47] There is no legal requirement in the U.S. for commercial websites or online service providers to maintain privacy policies. Due to the absence of data protection legislation, U.S. companies are adopting alternative means of assuring their customers of proper privacy practices. Third party organisations, for example TRUSTe and WebTrust, promote privacy practices and many U.S. websites display a Web seal to signal their compliance with the privacy standards formulated by the organisation.[48]

[45] Legislation.gov.uk, "Data Protection Act 1998," 2012. [Online]. Available: http://www.legislation.gov.uk/ukpga/1998/29/section/1.
[46] V. Mayer-Schonberger and F. Cate, "Notice and consent in a world of Big Data," International Data Privacy Law, vol. 3, no. 2, pp. 67-73, 2013
[47] K. Jamal, M. Maier and S. Sunder, "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom," Journal of Accounting Research, vol. 41, no. 1, pp. 73-96, March 2005
[48] Ibid.

Volume 11, July 2020 ISSN 2581-5504

ii. Government Regulation approach

Many European countries have created strict privacy laws. Directive 95/46/EC of the European Council was issued on 24 October 1995. It deals with issues on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The UK Government was required to implement this Directive, which it did in the form of the Data Protection Act in 1998. It came into force on 1st March 2000. This totally replaced the previous Data Protection Act of 1984.[49]

The Information Commissioner, a British Government agency, enforces the privacy law. Any owner of a website based in the United Kingdom that collects personal information is required by law to inform the Information Commissioner and abide by the eight principles of the Data Protection Act.[50] The principles provide guidelines and specifications for collecting and processing personal data and all e-commerce websites are required to have a privacy policy that informs the website's visitors how data can be retained, processed, disclosed and removed in line with the principles.

PRIVACY & E-COMMERCE IN INDIA

In India addressing the various issues relating to e-commerce and regulating the same, the Government of India enacted the Information Technology Act, 2000 (IT Act) on June 2000, its implementation from October 2000 with the publication of Information Technology (Certifying Authority) Rules, 2000.

A. IT Act 2000

IT Act traces its base from UNCITRAL model e-commerce Act which was developed with the aim of encouraging different Nations to adapt similar kind of law for recognising e-transactions. UN model of law defines Basic concept of emails, electronic signatures, electronic documents and so on also it ensures the acceptance of electronic signature, electronic records at par with handwritten signature and paper records respectively. Further the Act led to amendment in provisions of *Indian Penal Code,* 1860, the *Indian Evidence Act*, 1872, *The Bankers' Books Evidence Act,* 1891, *The Reserve Bank of India Act*, 1934.

The IT Act's basic framework is of UN e-commerce law. The Preamble of the Act states that; "Act to provide legal recognition for transactions carried out by the means of electronic communication, commonly referred to as 'electronic commerce' which involves the use of alternative to paper based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies"[51] The Act not only gives legal recognition to Electronic records and digital signature but it also talks about securing the

[49] G. Steinke, "Data privacy approaches from US and EU perspectives," Telematics and Informatics, no. 19, pp. 193-200, 2002

[50] K. Jamal, M. Maier and S. Sunder, "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom," Journal of Accounting Research, vol. 41, no. 1, pp. 73-96, March 2005.

[51] The *IT Act*, 2000, Preamble

same. Section 2 of IT Act provides the definition of cyber security; "Protecting information, devices, equipment, computer resources, computer devices and information stored there in from an authorised assess, use, disclosure, disruption, modification or destruction."[52] The IT Act 2000 is silent on many types of cybercrime, but it explicitly deals with few category of Cyber crimes that are;

I. tempering with computer source code;
II. Hacking;
III. publishing any information which is obscene;
IV. breach of privacy;
V. misrepresentation;
VI. Publishing digital signature which is falls in certain particulars or fraudulent act.[53]

As it clearly visible from its Preamble that the act's main objective is to build reliable electronic atmosphere which it is creating by providing electronic authentication. The Act on whole has lots of drawbacks as it itself doesn't covers the prominent cyber crime such as cyber stalking, cyber harassment, cyber defamation etc. It also provides way limited data protection through its sections on cyber contravention talking about unauthorised access to computer system or network.

Section 65 to 78 of IT Act deals with offences and prescribes the form of punishments for the cybercrimes specified in the Act. The Act also deals with damages done as civil offences, the different penalties have been provided for different type of damages. Currently IT Act had made necessary legal and administrative framework to promote the growth of e-commerce and e governance. It seeks to build confidence among the people that any wrong done in cyberspace will never go unpunished.

B. Payment and Settlement Service Act, 2007

This Act covers different payment systems used for financial transactions in India like; Real Time Gross Settlement (RTGS) system, Electronic Clearing Services (ECS Credit), Electronic Clearing Services (ECS Debit), credit cards, debit cards, the National Electronic Fund Transfer (NEFT) system, Immediate Payment Service and Unified Payments Interface (UPI), etc. The Act is regulated by RBI. The PSS[54] Act, 2007 provides for the regulation and supervision of payment systems in India and designates the Reserve Bank of India (Reserve Bank) as the authority for that purpose and all related matters. Section 2 of the Act defines "a payment system; to mean a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange. It is further stated by way of an explanation that a "payment

[52] The *IT Act*, 2000, Sec. 2(nb)
[53] The *IT Act*, 2000.
[54] Payment and Settlement Service Act.

system" includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations."[55]

C. National E-Commerce Policy

The Department for Promotion of Industry and Internal Trade under the Ministry of Commerce and Industry had released the draft for National E-Commerce Policy in February 2019. That draft has yet to be ratifying into a law. The main objective of National E-Commerce policy is to deal with the major issues related to the e-commerce i.e.;

I. Data;
II. Infrastructure development;
III. e-commerce marketplaces;
IV. Regulatory issues;
V. stimulating domestic digital economy; and
VI. Export promotion through e-commerce.

Also the draft for Personal Data Protection Bill, 2018 is under consideration.

D. CERT-In

The Indian Computer Emergency Response Team (CERT-In) was formed in 2003 to be the part of international CERT, with the set of approach to respond any security incident reported by computer and network community in the country. The mission is to enhance the cyber security in India and improve the infrastructure by pro-active actions and effective collaboration.[56] Its main aim is to become India's most reliable agency for being pro-active in relation to cyber security; whenever incident occurs.

SECURITY OF PRIVACY IN E-COMMERCE

People inevitably tend to group these concepts together. As online users seem to be more familiar with security technologies and thus, tend to perceive these as more important in an online framework.[57] Although they are interrelated, there are clear distinctions between the two concepts: While privacy is linked to legal require ments and good practices regarding the management of personal data, security refers to the technical aspects of this management and protection.[58] Protecting user data from online fraud can not be achieved without proper security. Nevertheless, consumers, companies and even official legislative bodies often view these concepts as very similar, and some authors have therefore proposed that they are two

[55] The *PSS Act*, 2007 Sec. 2(1)(i).
[56] K.Bajaj and D.Nag, E-Commerce; the Cutting Edge of Business, Second Edition, Tata McGraw Hill, New Delhi, 2011.
[57] Roca, J.C., Garcia, J.J., de la Vega, J.J.: op. cit., pp. 107
[58] Flavián, C., Guinalíu, M.: op. cit., pp. 604.

dimensions of a construct called SHPD: security in the handling of private data.[59] Customers, however they view these concepts, will usually care mostly about their data being protected, whether this is done by security measures or a company's policies. Security, as we have seen, relates to the ability of a company to protect its consumers online and prevent online fraud through security measures. Security involves both managerial and technical measures: the organizations' limitations of who can access the data within the organization and the purpose of this access. The technical measures include elements, such as encryption in the handling of the data, data storage on secure servers and the use of passwords.[60] Security is achieved if the information reaches the person without data being observed, altered or destroyed.[61] In more detail, this means that the transmitted or stored data can not be modified by third parties without permission; data can only be seen by authorized individuals; and certain actions can only be undertaken if proper authentication has taken place.[62] As with privacy, online users are usually aware of the fact that a company can never fully guarantee security. Non-expert users will not fully comprehend the scope of the technological measures on a website but will react to the perceived strength of a website's security.[63] The perceived security refers to the consumer belief that their personal data, including financial details, will not be abused. Though there are still many threats online, the technologies of e-security have advanced to the level where security breaches have been reduced.[64]

CONCLUSION & SUGGESTIONS

The growing trends of e-commerce there is simultaneous rise in menace, online frauds, hacking, phishing, cyber warfare like illegal activities are coming into frame. To curb this growing menace and bit the problem in its bud only, many legislations in different countries came into force from time to time. As we see there are certain minor difference among the Acts and policies of different countries but the major similarity exist that is the object and purpose of every law is common; to protect the rights of the online users, to provide them secure environment to access the digital world, to gain trust over the digital market by feeling safe not worrying about their privacy. Similarly India also brought its own legislation on the bases of UNCITRAL model to give legal recognition to electronic commerce as mentioned above. To give legal status to electronic signatures and records, while it has been successful in setting up the framework regulation for the same and addresses few misuse of technology, it has some lacunas too. It's been argued that it is a toothless legislation; there are some fields that require attention which it lacks. Spamming, Phishing, Data Protection in Internet Banking the main concern issues are not there in the Act and neither there is any separate legislation to govern them, as we can see in case of The USA and the European Union they have enacted anti-spam legislation. In fact, Australia has very stringent spam laws under

[59] Ibid.
[60] Shalhoub, Z.K.: op. cit., pp. 272
[61] Ramnath, K., Chellappa, P., Pavlou, A.: op. cit., pp. 359
[62] Flavián, C., Guinalíu, M.: op. cit., pp. 604.
[63] Arcand, M., Nantel, J., Arles-Dufour, M., Vincent, A.: op. cit., pp. 152
[64] Ibid.

which the spammers may be fined up to 1.1 million dollars per day[65]. U.K has more than 12 year old data protection law, under which banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection in respect of data. India doesn't have any legislation specially relating to the privacy laws, though concerns regarding privacy issue are at its peak. This is also serving as an obstacle in ecommerce as it is resulting in a loss of substantial foreign investment and other business opportunities. India is the host and the biggest platform of data outsourcing. It needs an effective and well formulated way outs to deal with these crimes. It needs to work more for enduring an effective and concrete legislation for data protection.

In the era of globalization and the age of e-commerce, technology is playing a significant role in the development of the economy. Through the global highways of information has given the new and different dimension to concept of information. E-Commerce has added wings to this new revolution by changing the pattern of business. Within the period of 20 years e-commerce established as a new dimension in the world of economy, where the information is considered to be the biggest and important asset. India, having the second largest population in the world, with a young, consumer oriented society, is emerging as a virtual treasure trove of information. In India, the Electronic Commerce market has been witnessing consistent growth in recent years. Despite the high rate of growth of e-commerce in India, the sector is still at a nascent stage and according to some estimates, it is about 3 per cent of the retail market worthUSD860 billion, excluding travel and tourism.[66] India is third largest internet user base country, even in proliferation of smart phones it is third largest country. In India transitional phase is going on, there is increase in the role of private sector, financial transactions are becoming digital. The country is moving towards the direction of e-governance, digitalization; Digital India initiatives like Sugamya Bharat Abhiyan, BHIM, COE-IT, CERT-In, DigiDhanAbhiyaan, Digitize India, Ebiz, Electronic Development Fund and GeM have been introduced by the government to facilitate commercial activities through electronic medium. India has stepped in to world's largest citizen identification program now that is Aadhar UID, sophisticated ID programme in the world. In this program all information related to an individual is captured like finger prints, retina image, address, birth proof and all. All these initiatives are taken to bridge the technology and coordination gap between the stakeholders of a commercial activity, to secure Indian cyberspace and to improve business environment by enabling fast and efficient access to government services through online portals[67]. All this signifies that India is the notable part of global digital revolution. While digital commerce is becoming an indispensable part of modern lives, it is important to

[65] https://www.lawctopus.com/academike/critical-appraisal-information-technology-act-2000/, last accessed on 20-11-2019.

[66] Draft National e-Commerce Policy; India's Data for India's Development, 2019; *at* https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf, last accessed at 17-11-2019.

[67] Draft National e-Commerce Policy; India's Data for India's Development, 2019; *at* https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf, last accessed at 17-11-2019.

Volume 11, July 2020 ISSN 2581-5504

consider issues relating to it. Country needs to have a strong strict and robust legislation to deal with the issues like privacy, security issues like phishing, cyber warfare, etc. There is an urgent need to strengthen the institutional capacity of an administrative organisation at digital level, to secure the sensitive contents because For instance once not only the site of National Information centre (NIC) was hacked, even the website of Ministry of Defence was also hacked. Programmes for cyber awareness need to be conducted for People at both individual and organizational level because there is lack of awareness relating to the cyber security. The government departments were found using Gmail accounts to share sensitive departmental information rather than having robust specified network system. There is lack of trained professional to deal with cyber issues. Having multiple institutions for guiding single law is the other loop. There is needs to be comprehensive legislation or inter institutional coordination must be at its par. Legal framework need to be strict and robust. Some improvements that are required in the legislation relating to the same are as follows:

There is a need of comprehensive legislation that would deal with the privacy issues which is the centre point in the current era people are dealing with. The creation of privacy policy is need of the hour. By law, all commercial Web sites are must require to display a privacy policy. E-commerce businesses, apps, Web sites and various other commercial Web sites need to have clearly outlined policy that provides updated information on what information is collected and stored, how information is stored, whether third-party apps or services are given access to information, and so on.

Customers must be kept informed and should have right to choice. It is responsibility of concerned company's website to keep customers updated on their privacy policy and all related changes. They should always ensure that customers understand company's approach to data collection and storage, when they are shopping and when any policies are changed. Customers should be given choice by allowing them to change their own privacy settings to control how much data is collected and used.

The IT Act need to cover the list of major crimes that are still not in the act, also it should raise the quantum of punishment which is prescribed in the Act.

No doubt we have taken major step towards digital globalization, by initiating digitalization on the basic ground level, being the part of e-commerce, promoting it to level next. But at the same time this requires a full proof security system backing up by cyber laws, privacy policy, security policy, cyber technology to provide the secure environment to the users; consumers, organizations who are the part of e-commerce at various phases like e-transactions, buying, selling, providing or receiving services etc.