CONSUMER PRIVACY IN E-COMMERCE

By Priya Singh
From Amity law school, Noida

ABSTRACT
The amount of e-commerce transactions has grown exceptionally with widespread usage of world wide web and enhanced network system. The consumer privacy in e-commerce is of utmost importance in this scenario. Privacy is connected with individual’s freedom and choice of life which should not be interfered by any external factor. In this paper the privacy risks associated to consumer’s data in e-commerce have been discussed. The study tries to uncover some of the means through which data is collected, instances when these data have been abused and how are the legislations of certain major nations dealing with it.

Keywords: Consumer Privacy, E-commerce, Cookies, Data Protection.

1. INTRODUCTION
In the past few decades an exceptional growth has been observed in online marketplace, better known as e-commerce. Though e-commerce is generally associated with online shopping, it is a much broader concept. It comprises of various commercial transactions based on the digital processing and transmission of data, text, sound and image. These transactions are made both between a company and a consumer and between different companies.¹

With the evolution of electronic transaction, a significant advancement in technology network have also been witnessed, paving way for e-commerce ventures in collecting, storing and processing large amount of consumer data for their benefits. This action has raised public concerns and consumer awareness about online privacy. It has thus become essential for states to bring legislation which are concerned about consumer privacy and data protection.²

Categorization of privacy has often been done in two parts: information privacy and personal privacy. The process of collecting, storing, processing and releasing of data is considered as “informative privacy.” In era of digitalization there is a plethora information on individuals in databases. This gives rise to the necessity of regulating such information, one of the first steps towards it being the drafting of privacy principles by the Organization for Economic Co-operation and Development (OECD) in the 1970s. Personal privacy relates to privacy of an individual’s private space which is prone to easy invasion by those seeking to photograph, film and record in public and private places or government surveillance.³

There is a thriving market for personal data in this digital economy. The information’s are collected from individuals are sold at high prices to a third part without users being

² FEDERAL TRADE COMMISSION REPORT: “PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE”, 2000
³ Rebecca Lipman, Online Privacy and the Invisible Market for Our Data, 120 Penn St. L. Rev. 2016
aware of it. The current system not only risk private data of individual but also takes their ownership rights over their own information. Data exploitation by agency like Cambridge Analytical in recent United States general elections are a fine example of it.

In the midst of all-inclusive electronic communication and expanding industry pressure for standard electronic verification, the maintenance of consumer privacy has turned into a subject of growing concern. The chance of an "invisible person" seems to be most apparent in e-commerce, partly due to the vast range of data available and partly due to enormous cost expected for using this data for commercial reasons. Thus, making consumer privacy of particular importance in e-commerce. This paper intends to analyses the importance of consumer privacy and understand the threats to it.

2. PRIVACY
The supreme court of India in 2017, interpreted right to privacy as a fundamental right available to all its citizens under article 21 and article 19 of the constitution in the case of Justice K.S. Puttaswamy and Ors. v Union of India and Ors. However, long visible trail of data left behind citizens in digital navigation raises concern. Security of the data collected during various online activities is a major issue. Section 43A of the Information and Technology Act, 2000, "Reasonable practices and procedures and sensitive personal data or information Rules, 2011" have frequently been suggested as a provision which provide an outline for the protection of data in India.

In the current era of blooming information economy personal data has become its fuel. With the help of massive developments in communication and computing services large amount of data is shared, collected, stored and analyzed every day. Access to such vast information provides e-commerce with opportunities to discover trends and channelize the potential in their business dealings. Consumers traditionally have very limited idea as to the possible usage of possession of such data allows, thus have almost no ideas as to the privacy violation that could occur.

For a long time, it was believed that these stored data are used in targeted advertising, weblining and consumer profiling but it has recently come to notice that many of the e-commerce websites are involved in data trading. Consumers majorly have two kinds of concerns regarding privacy. First, they are afraid about the use of their personal data for unrelated transactions without their consent, such as sharing it with third parties. Second, they are concerned regarding the illegal access to personal data due to security breaches or lack of internal controls.

In the last decade, consumers have become more aware about increasing privacy concern and have demanded more control over their personal data, this has led many states to


7 supra
consider the necessity of legislation on e-commerce consumer rights protection.

3. INFORMATION COLLECTION

In this era of digitalization e-commerce ventures are faced with many complex legal issues most significant among them being consumer privacy. E-commerce websites require certain necessary personal information such as name, delivery address, credit card information for their functioning which is voluntarily provided by consumers. However, in addition to it, many sites or mobile applications try accessing personal contacts and browsing habits of consumers, this data is matched with other geolocation information to create a consumer profile. It is then used in advertising that shows product prices to consumer depending upon profile. 

Users are discriminated in terms of the products they see, those who have more expenditure record or want a product more are shown higher price, alternately reduced price is denied to those who shop on bargains resulting in vendors making no profit from them.

E-commerce companies might not always want to participate in consumer profiling or might not even be actively aware about the amount of information they are extracting but the sensitivity of data collected puts them under great liability risk. Information is disclosed either via server software of sites or by third party extraction.

A. Software Server

The most preliminary stage of personal information collection is when the users register or place an order to e-commerce sites giving away details like name, email address, phone number and credit card number which are required to process transaction. However, additional information is automatically recorded by server software such as web log of browsing habits: what pages consumers visit, the time span of those visits, purchases made, advertisements viewed and clicked, query terms entered in search engines, and the website that directed the user to the company's page. These software also capture customers IP address to gather more insight on them.

B. Third Party

E-commerce websites also allow third-party advertisers to places cookies on consumer hard drives. Cookies are alphanumeric identifiers that recognizes consumer browser. They collect information of the users browsing and sends the data back to the web server. It is often explicitly mentioned in many e-commerce terms of privacy that “We do not have access to or control over cookies or other features that advertisers and third party sites may use, and the information practices of these advertisers and third party websites are not covered by our Privacy Notice or this Interest-Based Ads page.”

As per a FTC privacy survey, even though 57% of the websites allowed third-party cookie

12 Supra
13 Amazon.in Privacy Notice, available at: https://www.amazon.in/b?node=6691071031
placement, only 22% disclosed this in their privacy notice. Advertising networks even use web bugs on website pages to add data to user profiles stored in cookies and to collect statistics about how many hits the site gets. Advertising systems also use web bugs in "junk mail" to determine how many users checked the emails and visited the link, to remove consumers from the list who did not access the marketing emails at all, or to synchronize cookies with their email address.

New forms of technologies are being developed to obtain more wide-ranging data on consumer behavior such as radio frequency identification, global positioning systems (GPS), Consumer Profile Exchange standard, Pentium III's Unique Numerical Identifier, P2P profiling etc.

4. Instances of Consumer Privacy Breach

4.(a) Amazon.com: Price Deception

In September 2000, Amazon.com announced that it has personal information on almost 23 million of its customers. A notification was released stating that it intended to make changes in its privacy policy so that this data is not bought and sold as an asset. Two weeks after this announcement consumers noticed strange price differentiation in Amazon’s DVD section. Some consumers belonging to different demography or using different web browser were shown relatively high price whereas others were shown lower cost rate. Amazon later clarified the incident by declaring it a price test to examine purchasing behavior in random price variation, though it did not mention for how long it has been going on and till when it will continue.

Consumers and journalist were not satisfied by this statement, they discovered that there was certain specific pattern in these price variations. It was argued that these price differentiations had taken into account the spending habits of consumers. Those users who were most likely to pay more or do impulsive purchases were shown higher price whereas consumers with limited expenditure record or new consumers were offered lower. The key to this differentiation seemed to be in cookies that website place on users’ devices to track their browsing. Some users had deleted these cookies on their device or were using browsers which did not allow cookies were getting bigger discounts. This reflected that Amazon was offering discounts to tempt first time users back and existing users were given less discount by tracking their purchase records. This incident reflected the discrimination that can occur with internal secondary use of personal data.

15 Lectures on “consumer privacy” by Harvard Law School,2001 available at: https://cyber.harvard.edu/olds/ecommerce/privacypaper.html#devtech
17 Ibid
4. (b) FTC v. Toysmart.com\textsuperscript{19}

Federal Trade Commission filed a complaint against the commerce website “Toysmart.com” in the federal court of United States. It charged that the e-commerce company was involved in the data selling business of its consumers information, even though it had expressly mentioned not to share any user data with a third party in its privacy notice.

Toysmart.com had put up an advertisement in newspapers declaring the sale of its assets, including its customers' records. It had put user information’s such as names, addresses, credit card numbers up for sale as part of its bankruptcy proceedings. The lawsuit, brought in District Court, asked for bar on the sale of confidential, private customer data collected on the Toysmart.com.

5. Policies of major legal system
5.(a) The Current Status in India
The development in technological abilities, storage capacity and network system provide e-commerce companies more extensive scope for collecting, storing and processing of data. This enables websites to create personalized marketing system, which on legal level creates a greater hindrance in personal data protection. Although India does not have any express legislations involved in the data protection right now. However, there are relevant legislations such as Information Technology Act 2000, the Indian Contract Act 1872 and the Consumer Protection Act 1986\textsuperscript{20} which deal with protection of consumer privacy in e-commerce.

The Information Technology Act, 2000 currently deals with issues of e-commerce. It is inspired UNCITRAL, Model Law on e-commerce 1996.\textsuperscript{21} It deals with instances of wrongful revelation and misuse of private data and violation of contractual terms in relation to personal data.\textsuperscript{22} Though these laws regulate e-commerce presently but they are general and ambiguous regarding consumer privacy. Victims of data leakages from e-commerce platform often suffer while merchants enjoy with the ownership of vast amount of data.\textsuperscript{23} These situations therefore raise the question for specific legislation regarding consumer privacy from government. Construction of a codified law on data protection has been initiated in India and is likely to be introduce in near future.

5.(b) European Union
The European parliament had voted for the General Data Protection Regulation (GDPR) in 2016, which proposed to curb abuse of personal data and reinforcing the defense of personal privacy, came into force in 2018. After the implementation of GDPR, over 500 million people of European Union came under its protection. Although the UK had left the European Union, GDPR has still

\begin{itemize}
\item \textsuperscript{19} FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. filed July 10, 2000) available at: https://www.ftc.gov/sites/default/files/documents/cases/toysmartcomplaint.htm
\item \textsuperscript{20} The Consumer Protection Act 2019 was passed by the Indian Parliament in August 2019 and was to be brought into regulation in April 2020 but due to the COVID-19 pandemic it got delayed.
\item \textsuperscript{23} Guorong Zhong, “E-Commerce Consumer Privacy Protection Based on Differential Privacy”, Journal of Physics: Conference Series, 2019
\end{itemize}
officially been in the country. 24 It is considered to be one of the historic shifts in personal data protection in Europe. As per the provisions of GDPR, e-commerce companies are required to obtain consent of consumers in collecting, storing and processing their personal data, and consumers are to be provided complete ownership or control over their data. This act is applicable not only on the companies within European but even on foreign companies that deal with data of citizens from the European Union. GDPR provides certain significant rights such as the right to be forgotten, the right to restrict processing and the right to transfer data, which provide protection of consumer privacy on e-commerce platforms.25

5.(c) United States

The United States has multiple sector-specific and medium-specific national privacy and data protection laws, including those apply to financial organizations, telecommunications ventures, personal health data, credit report information, children's data, telemarketing and direct marketing.26 The US Privacy Act 1974 provides that:

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to agency, except pursuant to a written request

by, or with the prior written consent of, the individual to whom the record pertains.27

There are various exceptions to it, including the statistical reasons of the Bureau of Labor Statistics and Census Bureau, law enforcement reasons, archival reasons, congressional investigations and other administrative reasons.28 All US federal government agency are expected to place an administrative and physical security system to avoid unauthorized release of personal data.29

The Privacy Act was amended by the US Computer Matching and Privacy Protection Act 1988 to include protections for the subjects of Privacy Act records which are used in automated matching programs. It is designed to ensure procedural uniformity in carrying out matching programs.30


24 Ibid
25 Christina Tikkinen-Piri, Anna Rahunen, Jouni Markkula, “EU General Data Protection Regulation Changes and implications for personal data collecting companies”, computer law & security review 34, 2018
27 Privacy Act 1974, 5 USC 552(a).
28 Joel R. Reidenberg,” Restoring Americans' Privacy in Electronic Commerce”’, Berkeley Tech,1999
29 US Computer Matching and Privacy Protection Act, 1988
and Fair and Accurate Credit Transactions Act (FACTA) 2003\textsuperscript{31}.

**6. CONCLUSION**

Huge developments in the information and technology system has brought great opportunities as well as obstacles to the field of e-commerce. In this advanced electronic era of mobile internet technologies, it has become incredibly convenient for data to be transferred, collected making it even easier for their abuse. Consumer privacy breaches has eventually become one of the greatest threats in today's society.

E-commerce websites in process of collecting maximum data for consumer profiling not only put individual information at risk but also makes it more prone to security breaches. With this paper an attempt has been made to highlight concerns regarding consumer privacy, methods use to invade the privacy and the stands of government of various states on the issue.

*****

\textsuperscript{31}Information Shield, “United States Privacy Laws,” available at: www.informationshield.com/usprivacylaws.html