A CASE STUDY ON PRIVACY VS SECURITY WITH REFERENCE TO ONLINE TRANSACTIONS

***Prof. Divya Bansal** ****Emil Suresh**

Introduction

In today's society, we are surrounded by various forms of technology that could be used for many different purposes. There are many theories that the government monitors our use of technology to gather information about citizens and to keep track of any suspicious activity. Although this may invade personal privacy, it provides more safety for citizens.

On the other hand, there is a large controversy about whether or not the government should have access to our personal lives even if it provides for the greater good. Some believe that the government should be allowed to access to information such as phone data and computer usage histories in order to prevent crime and investigate criminal activity, but on the other hand there are some who believe that this would be an invasion of our Constitutional Right. The objectives of the current case study is to analyse in depth about the various measures taken by the government and weigh its pros and cons with respect to the public and to analyse whether or not the government should have access to our lives, even if it is for the greater good.

The world has changed definitely over the most recent decade. We have seen awesome technological wonders, a portion of the best among them was Internet, Smartphones and PCs. These innovative instruments facilitated our everyday work and helped us play out our errands proficiently and viably.

In the event that we are to comprehend the significance of technology, we should first see how has technology been affecting us through the ages. Throughout the years The web has become impressively tremendous over the course of the years. The historical backdrop of the web(internet) can be followed from the 1950s. It began as the idea of packet network systems which started in a few software research facilities over the USA, UK and France.

Web was instituted from ARPANET which was a military venture in the US which was made with the goal of associating a few super PC locales in the nation over with another on the off chance that any of them was destroyed by an atomic blast.

Amid the 1980s a British PC researcher Tim Berners-Lee's examination at CERN Switzerland brought about the World Wide Web, a connecting hypertext records into a data network.

***Prof. Divya Bansal**
Assisstant. Professor
MBA Department
Adarsh Institute of Management & Information Technology

****Emil Suresh**
MBA Student
Adarsh Institute of Management & Information Technology

Web did not get wide notoriety until the late 1990's the place just the military and couple of academic and research foundations approached the web.

PRIVACY versus SECURITY

So as to comprehend what this contextual investigation is about we should first understand what privacy and security means and how is it related to each other.

Privacy : It in fact implies the capacity of an individual or gathering to separate themselves, or data about themselves, and subsequently convey what needs to be specifically.

Privacy consolidates the hypothesis of regular rights, and by and large reacts to new data and correspondence advancements that emerges. Privacy rights are interrelated with data innovation.

As indicated by Black's Law Dictionary "right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned".

As indicated by Alan Westin, Privacy and Freedom, 1968-

"Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives."

As per the Article 12 of the 1948 Universal Declaration of Human Rights:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

SECURITY: Security implies the level of imperviousness to, or insurance from, hurt.

The most regularly known part of security is National Security.

National Security basically implies that the administrations with its parliaments, ought to ensure the state and its subjects are protected against a wide range of national emergencies through an assortment of energy projections, for example, political power, strategy, military may, financial power and so forth.

Humans have a characteristic need to control over classified piece of their life and this need has been perceived as basic ideal to protection. It is not a privilege against physical controls but rather it is a privilege against mental limit of right. The USA, UK, India, and among the International Level Universal Declaration of Human Rights, European Convention on Human Rights, International Covenant on Civil and Political Rights has perceived security as a basic right. Different judges and researchers have discovered the need of this privilege.

Indian Constitutional Provision:

The definitive law in India is the Indian Constitution. It is the longest composed constitution on the planet. It was drafted under the drafting board which was led by Dr. B.R Ambedkar. The Indian Constitution sets out the system for characterizing central political standards, builds up the structure, techniques, forces and obligations of government establishments and sets out basic rights, mandate standards and the obligations of the subjects.

The Indian Constitution as we see now has been affected from the accompanying

constitutions over the world: -

a) British Constitution.
b) United States Constitution.
c) Australian Constitution.
d) French Constitution.
e) Irish Constitution.
f) Constitution of Soviet Union.
g) Canadian Constitution.
h) Constitution of Germany.
i) Constitution of Japan.
j) Constitution of South Africa.

ARTICLE 21 of the Indian Constitution states that: -

"No person shall be deprived of his life or personal liberty except according to procedure established by the law"

As governments respond to weight from citizens, companies, specific interest parties, and overseeing methods of insight, we are seeing an assorted arrangement of security and protection directions. Some European nations, are centred around buyer protection and incorporate stringent prerequisites for revealing security ruptures. Others are worried about digital assaults from criminals, or from fear mongers and country states, regardless of whether they include the burglary of protected innovation, assaults for monetary benefit, or vandalism to disturb financial movement or physical framework.

Various countries have distinctive bits of knowledge to directions on how the web can be utilized and it likewise has different directions with respect to the administration control over the checking of their countries web movement.

As the characteristics of a coin, technology has two sides. One which is the instruments utilized for more note worthy's benefit of humankind and the other for the devastation of mankind.

With this being said the inquiry emerges in regards to well being and security of technology driven gadgets alongside the protection that specific advancements accommodate its clients. The World Trade Center assault was the single greatest disaster that set off the war against fear based oppression group all over the world and the stringent establishment of digital laws and counter digital psychological warfare. Every country has diverse sorts of digital laws and counter digital fear based oppressor measures. A standout amongst the most normally utilized measure by every one of the legislatures over the world is reconnaissance/ surveillance of their citizens and nation.

ANALYSIS

Data protection has been a sensitive point especially after exposures by past National Security Agency legally bound worker Edward Snowden about the level of the US governments observation exercises.

Lately the most prominent security breaks have focused on credit card numbers, individual photographs, or diverse bits of put away information. Regardless, we don't consider the extending volume of data that we are of all aims and reason giving without end, paying little respect to whether adventitiously or by communicated consent. Every last one of us has a mobile phone and every one of us approaches the web and diverse applications that we use on our phones, yet a substantial part of us doesn't consider what data is assembled by each of the applications on our phone, regardless of whether it is sent? furthermore, who is using it? A considerable measure of this information may be contained in the 24-page end-user license agreement (EULA), yet really 98% of us ordinarily click acknowledge without endeavouring to seek after it.

RIGHT TO PRIVACY IN INDIAN SCENARIO

Article 17 of the International Covenant on Civil and Political Rights states about the privilege to security, it expresses "Nobody might be subjected to self-assertive or unlawful obstruction with his privacy, family, or correspondence, nor to unlawful assaults on his respect and reputation". While Article 12 of the Universal Declaration of Human Rights 1948, states "Nobody might be subjected to discretionary impedance with his privacy, family, home or correspondence, nor to assaults upon his respect and reputation. Everybody has the privilege to the insurance of the law against such obstruction or assaults". The two instruments give the privilege to security to the subject, and the states, who are signatory to it, are relied upon to satisfy these rights.

Since India is a signatory to the International Covenant on Civil and Political Rights and Universal Declaration of Human Rights, 1948, India has the commitment to implement these rights.

In the absence of empowering enactment, the ICCPR can have the legitimate power as alternate laws in India. Also, the UDHR is a simple assertion, and it doesn't have the lawful power. Be that as it may, the courts have utilized arrangements of ICCPR and UDHR to make its contention more grounded; and furthermore so as to make understood the administration about his commitment toward it subject and towards worldwide instruments.

CURRENT SCENARIO

In the event that we investigate the smartphone market in the nation today, we see that greater part of the telephones sold in the nation are made in China or have their beginnings followed back to China. The administration feels that the current increment in strains amongst India and China will prompt a point where crucial information of different people will be bargained and could be accomplished unlawfully.

The administrations concern starts from the way that lion's share of the web used in the nation is done through cell phones. After demonetization, the administration has helped to support online exchanges in the country which has prompted and over drive in the field of computerized exchanges. This huge lift in computerized exchanges has offered ascend to dread of guiding of information and hacking to a basic level. Voicing its worry, the Indian government as of late reported its preparing to set obligatory strict security and protection rules for smartphone producers. This choice by the government is a noteworthy turning point in the security of client's protection access by different outsiders. Other than guaranteeing security of client's information this development by the legislature likewise goes for controlling the stream of individual data to different servers abroad.

Financial and individual informational collection aside, the government administration fears that the data achieved illicitly will incorporate the person's medical records, locations, their perusing history and so forth. This choice to command strict directions on information protection and security originate from the legislature amid the time where the administration has issued notice to very nearly 30 organizations on worries on cyber security. Among these 30 organizations likewise incorporates Chinese handset makers Gionee, Oppo, Vivo, Xiaomi, Huawei and One Plus. Aside from Chinese handset producer’s different organizations like Apple, Samsung, Lava, Karbonn and Micromax has additionally been served the notice from the government. The notice from the administration covers the

worry of security which incorporates the gadget, its working framework, program on the gadget and preloaded applications.

2017 Supreme Court Judgments

The Supreme Court on August 2 2017, laid out a three-level, evaluated way to deal with the inquiry whether security is a principal ideal by looking at the issue through its Intimate, Private and Public perspectives even as it saved its decision for the situation.

Preceding completion of the two-week-long hearing that pulled in contentions for and against giving basic right status to security however which saw all gatherings tolerating its inherent significance for an individual, a nine-judge seat headed by Chief Justice J S Khehar said protection could be designed into three zones.

As according to Justice D Y Chandrachud "The primary zone could be the most personal zone of protection concerning marriage, sexuality, relations with family and the law should disapprove of any interruption. The state could at present barge in into this zone in phenomenal conditions gave it met stringent standards.

The second zone would be the private zone, which included separating of individual data+ by usage of credit card, social network platforms, income-tax revelations. In this circle, sharing of individual information by an individual will be utilized just for the reason for which it is shared by a person.

The third is the general population zone where security insurance requires negligible direction. Here, the individual information shared won't mean the privilege to security is surrendered. The individual will hold his protection of physical and mental state."

As of late on August 24 2017, the Supreme Court of India set an order that will influence all of the Indian citizens that number at 134 crores. The zenith court decided that Right to Privacy is a Fundamental Right. The judgment of Right to Privacy is a Fundamental Right, the court has overruled past judgments on the security issue. The apex court expressed that Right to Privacy is crucial as it is for the Right to life and additionally the whole Fundamental section of the constitution.

This decision by the apex court of India is an aberrant hit to the administration push to make Aadhaar obligatory for every one of the Indian citizens.

This stupendous decision was finished by the nine-judge bench whom overruled the past judgments on the issue alongside the eight-judge bench judgment in the MP Sharma case and the six-judge bench judgment in Kharak Singh case wherein both the eight-judge bench and additionally the six-judge bench had decided that Privacy is not a crucial right.

The established status of Right to Privacy came into to light in a pack of petitions drove by previous High Court Judge K S Puttaswamy in 2012 where the request of tested the UPA government 's choice to present the biometric information empowered Aadhaar ID for the residents. Different solicitors additionally incorporated the principal administrator of National Commission for Protection of Child Rights and Magsaysay awardee Shanta Sinha, a conspicuous women's activist scientist Kalyani Sen Menon. The candidates say that The Right to Privacy is "natural" and "characteristic" to the most imperative crucial right that is The Right to Liberty. Likewise, the Right to Liberty additionally included Right to Privacy was a previous part. This implies the constitution recognized and ensured to the nationals in the event of infringement of rights by the state.

When we analyse the Right to Privacy, we can see that the Right to Privacy contains several Sub - Species. This implies that it is intrinsically impermissible to pronounce every single example of privacy as a key right. It is best to decide independently the different parts of privacy and the degree of infringement that could trigger a protected constitutional solution.

Following the decision by the supreme court of the country, the current government of India and in addition all the political organizations has respected the courts choice of the need to privacy a fundamental right collectively. Despite the fact that the government administration has respected the choice they are it the viewpoint that the privilege to protection ought to be liable to sensible confinements. It ought to be liable to sensible limitations as is with whatever remains of the rights ensured by the Constitution of India.

The law minister has stated that privilege to security is not a flat out right and it has its confinements. It must be recognized by case-to-case premise. These being that protection ought to be liable to sensible confinements which the state has chosen to entitled on the premise of social, moral and convincing open enthusiasm for agreement with the law of India.

The supreme court has perceived the need and significance for the vigorous information regime to adjust delicate worries between singular intrigue and state intrigue. In light of the current supreme court judgment the government has framed a powerful advisory group for information protection and security.

EFFECTS OF RIGHT TO PRIVACY

The nation’s apex court judgment has a significant affect on the fate of Aadhaar and the LGBT community.

1) Aadhaar Section 377

At present the court is as yet inspecting the legitimacy of Aadhaar in wake of the current judgment on the privilege to security. It is likely that the Aadhaar will stay dynamic yet under an arrangement of clear and dynamic rules with respect to its utilization. The current decision has empowered the government to gather information from the citizens without being blamed for disregarding privacy in the event that it is done for the National Security or for viable circulation of rare national assets, nourishment and other fundamental things.

SOLUTION

Companies actualize security efforts to ensure safety of digitally transmitted data. The government orders security of individual data in the medical and budgetary administrations enterprises. While on the flipside, government bargains protection and requests access to ensured data for the sake of maintaining national security.

At the point when government authorities discuss security, they're looking at shielding the overall population from dangers, (national and international). Their objective isn't to profit or to radiate trust among clients, but instead to prevent the terrible folks from doing awful things. It might sound deceptive - rebuffing the great individuals to get a couple of awful folks, yet the government contends that relinquishing some affable freedoms is important to ensure against the danger of terrorism. This implies there are circumstances where security wins over privacy. The problem in security and protection is not constrained to law enforcement authorities and people. Companies are additionally confronting the security-protection problem. For instance, the reliably demonstrated data shows that one of the greatest security dangers confronting

companies is from insiders, who are the workers who abuse or manhandle rights they are given to carry out their employments. Moreover, courts have held companies subject for abuse of their IT assets, driving numerous associations to screen their representatives' utilization of email and the Internet. As per the American Management Association, more than 80 percent of the organizations it overviewed utilize some type of electronic observing or reconnaissance to watch their representatives.

Notwithstanding, there's a developing pattern for courts and councils to perceive the privileges of employees to workplace privacy. In a current case, a court found that it is illegal for the company to take a gander at a worker's email if it's marked "individual." If this pattern endures, it will place organizations in an impasse where they will be presented to risk regardless of whether they screen workers action. A large portion of these contentions can be kept away from if every circumstance was examined from both a protection and a security point of view.

The private sector additionally confronts many difficulties in the current calls for more open public-private comradeship in battling terrorist activities on the Internet. While this kind of organization has stupendous potential, there will without a doubt be a few hindrances. For instance, organizations approach security from a business point of view. Law enforcement authorities doesn't think that way. Asset limitations do require prioritization, however that is not the same as the hazard administration examination of the private part.

CONCLUSION

The immense growing development of Internet is compelling more consideration on the issue of Privacy and Security, and arrangements are approaching or officially accessible as IoT Gateways, chip-based security, secure boot records, and encryption, among others.

There are regular and unavoidable clashes, reflecting the hundreds of years old open deliberations between promoters of national and business security and supporters of privacy and common freedoms. The most ideal approach to determine them is with more joint effort and, trade off amongst security and privacy. Many clashes can be entirely avoided if public sector and private sector cooperate to guarantee that security and privacy contemplations are tended to and satisfactorily spoken to all phases in the advancement of computer frameworks, corporate approaches and government directions.

Sadly, you can be consistent without being secure, and without doing any more for privacy. Over and over again, the objective of a security venture is consistence, and the undertaking reports are separated from the genuine security stance or privacy abilities.

In my perspective, security prompts privacy, which prompts consistence, not the opposite way.

REFERENCES

- Assembly, U. G. (1948). Universal declaration of human rights. UN General Assembly.
- Breaux, T., &Antón, A. (2008). Analyzing regulatory rules for privacy and security requirements. IEEE transactions on software engineering, 34(1), 5-20.
- Campbell, H. (1990). Black's law dictionary. St Paul Minn: West Publishing Co.
- Cavoukian, A. (2011). Privacy by design in law, policy and practice. A white paper

for regulators, decision-makers and policy-makers.

- Flaherty, D. H. (1989). Protecting privacy in surveillance societies (p. 306). Chapel Hill: University of North Carolina Press.
- Flavián, C., &Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Industrial Management & Data Systems, 106(5), 601-620.
- Nissenbaum, H. (2004). Privacy as contextual integrity. Wash. L. Rev., 79, 119.
- Pfleeger, C. P., &Pfleeger, S. L. (2002). Security in computing. Prentice Hall Professional Technical Reference.
- Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: a survey study. Information Management & Computer Security, 9(4), 165-174.
- Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166.