MSB- INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEACH
ASSOCIATING RESEARCHERS; NOURISHING INNOVATION
Peer Reviewed
Vol. 1, Issue 2, Dec.2022- Feb.2023,
08-14, MSB-IJIR

NETIZENS DATA SAFETY & PRIVACY PROTECTION

Mr. Ayush Saran Assistant Professor, Amity Law School,
Amity University Lucknow
asaran@lko.amity.edu

Abstract:

"**Even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of the right**"([1]Grswold v. Connecticut (381 U.S. 479. 85 S.Ct.1678,14 Ed.2d 510 1965).

Today the data available on the internet when classified into information helps in the better communication but the tools used for cost-saving benefits, efficiency of network programming often result in creating new challenges to the privacy and data security of the entity to which data is money in economic context. In view to cater these new challenges of cyberspace the information technology professionals are building the aspiration of the people towards concepts of cryptogenic data storage technology, cloud computing end to end inscription programming in order to create a social dilemma of best security of there platform.

Keyword: Data Safety, Privacy Protection, Law, Internet, Society

Introduction:

The Internet is a collection of technologies and an international network of networks, each of which engineers have invented and developed for their own work and to serve specific purposes. It is made up of a number of different ways to organize, transmit, and access information. It is unlike any other medium, because of this multiplicity of systems. The emergence of the artificial intelligence tool to limit or codify our preferences into the network and application memory to affect human thinking in a particular direction is also creating bug of dumbness of the human mind into machine driven neurology which in times to come will affect our intelligence quotient.

Taking into consideration the amount of data uploaded by individual users on the internet, the need for privacy-enhancing technologies has become a basic need today to secure the cyberspace. Electronic mail and electronic fund transfers, for example, should provide a safe means of encryption and authentication, which can only be done if third-party storage is abolished and cryptographic technology knowhow is readily accessible and unencumbered by government regulation. Furthermore, whether or not government enforcement of cryptographic security techniques endangers an individual's personal privacy can still be determined using the privacy protections available to people.[2] (Claypole, T. F. (2004). Privacy Regulations a Concern with Internet. Retrieved November 6, 2022, from http://gilc.org/crypto/crypto-survey.html). Encryption provides individuals with the assurance that no third party will be able to get through the wall of a self-instructed programming computer. usage of the right to free speech and expression, as well as the right to hold a private conversation without being interrupted.[3] (Privacy International. (n.d.). Responding to Terrorism. Retrieved November 6, 2022, from http://www.privacyinternational.org/article.shtml?cmd [3])

The fact that cyberspace is marked by less governance and poor rule of law, such as the international transmission of a large number of data drive-by attackers using key loggers on social media to other countries where cybercrime law was nascent and non-existent or not easily enforceable, is part of the internet's fascinating character. Although the severity of cybercrime has been recognized by countries around the globe and many of them have taken legislative measures to assist greybeard and offenders, not all have a legal structure to facilitate cyber criminals' prosecution.

Globally many developed and developing countries have also reviewed their respective domestic criminal legislation to avoid computer and cyber-related crimes in order to address the

challenges raised by emerging forms of cybercrime and criminal profiles. The government also makes regulations ensuring that internet policies and security solutions are in place for any enterprise from a large corporation to mid-size and small ones. In view of the dynamic and rapidly changing technology, there are often new types of threats. Cyber attacks, though, are moving at a high speed that law enforcement will not capture the day in the latest pattern, then corporate individuals will begin to think twice about using social network sites and the Internet.

PRIVACY IN THE OPEN INFORMATION SOCIETY

Internet Privacy

Privacy is a multi- dimensional concept that includes physical privacy, information privacy, social and psychological privacy. In the online environment, netizens have become an object of surveillance. The new internet-based technologies are not only increasing their capacity to collect and process data, but are also changing the dynamics surrounding the collected information. Privacy is considered as a part of the vocabulary of every society. It is a human value enshrined in human behavior which goes with human desire. It preserves and protects human autonomy under the umbrella of human dignity. Privacy as a basic feature touches humans upon fundamental needs and values associated with men's gregarious nature. Certainly, the level of technological and economic blueprint creates pressure to protect these privacy values through legal enforcement techniques. It has been traditionally considered legal enforcement techniques.

It applies to acts of violation on the internet that are of a commercial nature and not solely due to the offender's motivation. Although some internet pirates generate revenue from their actions, for other non-commercial purposes, many individuals participate in such acts and all of them in order to cause enormous commercial harm. As we progress further into the technological advanced era of human existence, the influence and reach of the internet only continue to expand. With this expansion of technology, there will be an increase in the virtual space privacy.

Privacy has been one of the most valuable possessions of man since ancient times. Over a period of time, its increasing importance was recognized and concern for its security was never so crucial as in the age of information technology. The right to privacy can be defined as a person's right to enjoy his own presence on his own without the boundaries of physical, mental

intrusion from other individuals. Presently several types of surveillance system by governmental authorities are being operated but they are devoid of any concrete legislation and they take their validity from vague notions which are sheer violation of human rights besides this we have no concrete framework to counter data related issues which is open to be violated. Apart from this with the advancement of time and technology new issues have also emerged but what about new issues where old issues are still to be tackled.

International Conventions

Our civilization has progressed over the centuries, breaking down all territorial barriers, and the internet is the most notable contribution to human civilization in recent years, bringing the entire planet closer together and transforming it into a global community. However, cyberspace, a modern virtual village, has introduced new threats that bring into question the very nature of personal privacy. Some international conventions which widely discuss the issue are :--

Article 17 of International Covenant on Civil and Political Right,1966,

Article 16 of United Nations Convention on Protection of the Child, 1989.

Article 8 of the European Convention for the protection of human rights and fundamental freedoms, 1950.

These are some of the basic structure having wide scope of protection of the individual privacy and securing the identity of the individual.

In a 1902 event in the state of Georgia, the right was first recognized in the United States. After that time, individual claimants have also been allowed by courts in the United States and around the world to pursue legal remedies for private life invasions. The right to privacy in the area of information technology has centered on the ability of individuals to manage information collection. This was also defined by a German court as the right to "information self-determination". This right is also articulated and codified in civil law as fair practice of knowledge.

In international and national law, the right of privacy is well established. After the adoption of the Universal Declaration of Human Rights, 1948.Most governments have a general right to privacy set out in their constitutions at the national level. Privacy rights have also been

established by means of case law and by legislative enactments. Such laws usually aim to safeguard privacy in a particular sense, such as laws that protect communication privacy by restricting the circumstances in which police can perform wiretapping or when personal data can be sold by a retailer. Surprisingly, the unification of European countries and the establishment of the European Union has highlighted the fact that privacy is now firmly defined as a legal right. As a result, privacy security remains a top priority for governments in the twenty-first century, demonstrating the significance of this constitutional right.

What legal safeguards will help symbiotic development of Tech and Law

One of the biggest barriers to privacy security is only partially technological in nature. In this climate, it has become commonplace to clearly say that national governments will be unable to exert any legal influence over the Internet, and that existing laws will have no effect on the digital world. However, this viewpoint is incorrect in at least two ways. First, governments do exert a great deal of power, despite what the "cyber-intelligentsia" says. Internet conflicts are settled in real courts, and computer offenders are sentenced to real prisons. Second, the dependence on conventional legal institutions has not decreased as the Internet has become more commercial and popular. Since there are no formal adjudication methods in cyberspace, governments and private parties have inevitably switched to conventional methods of settling conflicts and prosecuting malicious actions. Finally, and perhaps most significantly, policymakers have discovered that if there are interests that should be preserved, concerted action at the supranational level can be taken to protect those interests.

How to Save Data and Protect Privacy[4] *(Data protection in the EU*. European Commission - European Commission. (2022, October 14). Retrieved November 6, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en)

The security level protocol of individual identity data should also be encrypted in a secure algorithm which should be controlled and secured by the national security system security agencies of the country to which the data belongs and which can only be accessed via their local server and cloud storage system. In countries where cyber security protocols are weak and a firewall framework for controlling internet traffic is established, the local area network for

country data sharing should be encouraged.

Although we should not minimize our efforts to ensure that privacy rights are effectively enforced across national boundaries, we should also not neglect the possibility that technology can offer certain privacy protection solutions. In the first place, what ensures anonymous transactions is the best method of privacy security through technical means. Anonymity is the perfect technology for privacy because it prevents the production and compilation of information that is personally identifiable.

CONCLUSION

Netizens of the cyberspace believe that everything is free here, but the truth is this new virtual reality has not been created by God but by humans and every human invention has a price to be paid by its consumer. Thus, the advertisement companies own the internet platform and earn the data of the netizens by the internet companies and in turn we (netizens) become the product of their sale. The purpose of all this is to convert the data into valuable information and channelize the business entity according to the advertiser product and store personally identifiable information (PII), such as address and date of birth of the netizens to sale human future aspiration according to their preferences. Issues occur when access to knowledge is extended by the transfer of rights beyond the group of friends. This is where the initial privacy takes place. The customer is, in many cases, unaware of the extent to which the PII has spread. The reality that social networks are still emerging is another reason. Until they reach a mature state, concerns about data safety and privacy will continue to pose issues.

In many contexts today, anonymity occurs by tradition and practice. We have come a long way on the road to data security, with the Supreme Court of India holding the right to privacy as a constitutional right. One will have to admit, though, that a great deal still needs to be done. A legal structure relating to the methods and purposes of assimilating personal data offline and over the Internet needs to be developed.

The National Commission to Review the Working of the Constitution[5] (Ministry of Law & Justice. (2002). (rep.). *Report on National Commission to Review the working of the Constitution* (Report 62). Government of India) recommended a constitutional amendment in the form of Article 21-B, which shall make "right to privacy" a fundamental right under Part III of the Constitution. The section would state as follows—

"Art. 21-B. (1) Every person has a right to respect his private and family life, his home and his

correspondence.

(2) Nothing in clause (1) shall prevent the State from making any law imposing reasonable restrictions on the exercise of the right conferred by clause (1), in the interests of security of the State, public safety or for the prevention of disorder or crime, or for the protection of health or morals, or for the protection of the rights and freedoms of others."

The Parliament has to undertake extensive legislation in order to deliver to Indians their paramount right of privacy.

REFERENCES

Grswold v. Connecticut (381 U.S. 479. 85 S.Ct.1678,14 Ed.2d 510 1965).

(Claypole, T. F. (2004). Privacy Regulations a Concern with Internet. Retrieved November 6, 2022, from http://gilc.org/crypto/crypto-survey.html).

(Privacy International. (n.d.). *Responding to Terrorism*. Retrieved November 6, 2022, from http://www.privacyinternational.org/article.shtml?cmd [3])

(Data protection in the EU. European Commission - European Commission. (2022, October 14). Retrieved November 6, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en)

(Ministry of Law & Justice. (2002). (rep.). *Report on National Commission to Review the working of the Constitution* (Report 62). Government of India)