VOLUME 3 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

PRIVACY ISSUES IN CYBERSPACE

- Chitra Dwivedi[1]

INTRODUCTION

Cyberspace means the virtual world of computers and gadgets where internet is involved, where individuals can interact, conduct business, do transactions and develop software's and graphics. The advancement in technology and internet has caused a revolution in the way how people connect and interact with one another. Nowadays, almost every person, every institution, every activity (private or government), every transactions is under the realm of cyberspace. The unrestricted freedom that internet as a platform has provided have allowed the peoples to share any information on social media websites, specific platforms and online institutions. The information can be very sensitive personal information or can be as general so that it can be seen public, which is of users concern.

But the more interconnection and more interaction in cyberspace means more availability to a person or institution to gather, store and process of personal information for any unconsented or illegal use of that data.Before the era of cyberspace, it was much more convenient to discover the source of any privacy infringement and fix the liability for the same. But in the cyberspace, the higher vulnerability, anonymity and jurisdictional issues have made it tough. The youth and teenagers are more exposed to it because high number of users consists of them and the unawareness among them of the exploitation and victimization in cyberspace. This can be challenging parameters of privacy to the person concerned. Privacy can be defined in terms as "**a right to be left alone**". The unrestricted freedom, abundance flow of data and the electronic footprints that a user left while each click and each browse, has left no information private. This can be used to know the sensitive data and interests of the user. These days, the privacy of a person in cyberspace seems to be a myth as many privacy threats and cybercrimes are been done using the

[1] Student at Amity University, Patna

data in not so proper and legal manner. The cyberspace's openness is thus in a direct battle with the privacy of a person.

Now the question whether the citizens are willing to surrender their sensitive personal informative publically or not is debatable but still it is the responsibility of legal domain to prepare proper policies, legislation and institutions to harmonise the battle. Right of privacy is a human right and recently it has been given a status of fundamental right though it not directly conferred by the Constitution of India. Thus the protection of it is a major and compulsory challenge. In this paper, we will try to identify the information privacy issues in cyberspace and the threat they possess. Then paper will further discuss and critically analyse the current legal status to eliminate those issues and the lacks in them. At the end, the paper will try to suggest some legal and institutional reforms that will strengthen the battle of legal domain against the privacy infringement.

PRIVACY ISSUES IN CYBERSPACE

In the domain of the cyberspace, the privacy of an individual can be easily compromised due to the easy flow of data and the anonymity of the persons making any unconsented/illegal advantage of it. The content in the form of any information uploaded and shared on the internet is permanently saved in the form of link and is available for reference by anyone who is able to trace it. The information of any kind may it be an email, the credit card details, the personal content like images and documents, the chats and messages in all formats etc. are all stored somewhere on the remote computer through which it may be accessed at any time and by anyone unless few safety measures are strictly followed.Thus netizens are thus at high risk of privacy infringement. Since the realm and nature of the cyberspace is a new world, the legal regulations are trying to catch up with the fast growing ambit of it but are still lagging in many ways. In this section of paper, we will try to identify some of the important privacy issues that occur or can potentially occur in cyberspace. Some of the important privacy issues in cyberspace are as follows: -

1. SPAMMING:

It is the method in which website preferences of the users are tracked and then unwanted messages like advertisements, offers and marketing of certain products are being sent to the users in bulk based on their tracked website preferences.

For example, a user visits an online shopping platform and searched for some shoes. Then his/her surfing on the website is tracked then the user has been sent the offers and advertisements to him through mails and messages based on his tracked preferences.

It can cause serious harming to a person's computer by infecting it with malicious software and can lead to damaging systems and stealing personal information. A spammed message can also contain viruses and spywares which can be used to obtain sensitive personal information from the computer resources.

It is a privacy infringement of an individual where the personal action of the user as well as his personal contact details is being tracked and being shared with the marketing agencies and other companies. It also leads to damaging of person's computer and stealing of its sensitive and uncompromised information.

2. COPYRIGHT INFRINGMENT:

Copyright is a legally conferred right to the person where he/she has an exclusive right to publish his/her works, to control copying of his/her work or product, to prepare derivative work, to make the material available online.

But this right has been most commonly and easily infringed in the cyberspace. The creative contents of an individual like photos, videos, arts and writings are being easily copied on the websites and social media and being used for commercial and non-commercial purposes. The thefts of data are very common these days because of huge flow of information.

The Copyright Act, 1957 prohibits the copyright infringement. But the amount of copyright infringements which are trivial and most common in nature can't be practically contested legally. For example, if a food blogger posts a 30 seconds video on his social media accounts and it has been copied by any user, it is practically not feasible for him to bring legal action against the infringer. The cyberspace makes it more complex as many users are anonymous who handle accounts from a fake identity.

Thus the copyright infringement (also called piracy in slang) is a common privacy infringement in the cyberspace and creates serious privacy problems to a large number of users.

3. IDENTITY THEFT:

Identity theft means electronically impersonating someone for the financial gain. It can be for example, by using someone else's login credentials to enter into a protected system. It is most commonly used by hacking the accounts of an individual who is using a unprotected website and app and then using his/her login details of banking and credits to gain some financial benefits.

It is a serious nature privacy infringement where even the most sensitive personal information can be stolen and cause serious financial and mental burden on an individual. It has been criminalize under Section 66C and Section 66D of The Information Technology Act, 2000.

4. CYBER STALKING:

It is a process in which a person (known here as stalker) tracks the activities of an individual on regular basis on the cyberspace and mostly in cyberspace by different ways like post following, noticing of personal details, downloading of pictures etc. It can also lead to online harassment and online abuse. While most of the victims of this infringement are women, men can also be the victims of it.

It is a gross infringement of an individual's right to life with dignity and honour. It kills the privacy of a person who "wants to be left alone". Though it has been criminalize under Section 509 of Indian Penal Code and Section 67 and Section 67A of the IT Act, 2000; still the practice is very common because of the reasons like anonymity of the users in cyberspace, non-complaint of such practices and non-awareness among the cyber users regarding stalking.

Case: Manish KathuriaVsRituKohli[2]

In this case, the petitioner was being stalked by the defendant for four consecutive days. The defendant was chatting illegally by using her name and used obnoxious and obscene words. He also distributed her contact number and invited them to chat. Due to this she started getting many calls in odd hours. Because of this she went in the state of shock and finally reported the case to Delhi Police. The accused was booked under sec 509 of IPC.

[2] C.C. No. 14616/2014

5. WEBSITE VANDALISM:

It is type of privacy infringement where there is the process of attacking and vandalizing the websites and replacing the hosted website by breaching into the web servers. The vandalism is done with the purpose of theft to data and information that the vandalized websites gets or has stored either of its own or by its visitors.

The vandalism is a serious infringement of privacy because here not only the data of website can be compromised but also the information and sensitive data that the users of the websites provides which may include the sensitive personal information can also get compromised.

The section 65 of The Information Technology Act, 2000 punishes for the website vandalism.

6. CORPORATE ESPIONAGE:

It is basically a process of spying where one company or organization spy on the sensitive information or companies strategies of another companies through electronic surveillance or data theft to gain some competitive advantages over others.

The corporate espionage can be done either by cyber-attacks, malware installation, Intellectual Property theft, or wiretapping. This can lead to serious privacy infringement as data stolen through this can be sensitive information of the victim company's customers or employees.

LEGAL PROVISIONS AND GUIDELINES FOR CYBERSPACE PRIVACY IN INDIA

The cyberspace is new and different arena comparably to traditional space thus requires different approach and laws for regulation. The kind of vulnerability of privacy infringement that exists in cyberspace is a challenge for the legal domain to overcome by introducing new laws, institutions and protective systems. As of now, there is no separate statute for cyber privacy in India but many provisions of The Information Technology Act, 2000 and IPC provides some safeguards to the privacy in cyberspace. Also some articles of Constitution of India, 1950 protects the privacy of individuals as a part of fundamental right. Further, some landmarks judgements in recent years have strengthen the stand of privacy like case of *K.S Puttaswamy v Union of India.*

Acommittee formed under Supreme Court Judge Justice Sri Krishna suggested making a legislation which is later drafted under the title as Data (Privacy and Protection) Bill, 2017 & 2019 but is still to be passed by the Parliament. Also some International Convention like OCED suggested some methods to be adopted by nations regarding protection of privacy and trans border flow of personal information but still it is unsanctified by the Indian Government .

The Information Technology Act, 2000

Many sections of IT Law, 2000 tries to criminalize the certain acts which can cause the privacy infringement and can exploit the data without consent. It also has certain provisions which prohibit cyber-crimes that compromise the data.

- **Section 43** provides for the penalty and compensation for the damages to computer and computer systems.
- **Section 66** provides laws for computer related offense.
- **Section 66C** dealt with Identity Theft and Hacking.
- **Section 66D** provides punishment for cheating by personation by using computer sources.
- **Section 66E** provides punishment for violation of privacy.
- **Section 67C** contains provision regarding preservation and retention of information by intermediaries.
- **Section 69** provides powers to issue directions for interception or monitoring or decryption of any information through any computer source.
- **Section 72** has provision regarding privacy and confidentiality.
- **Section 72A** provides punishment for disclosure of information in breach of lawful contract.

The Constitution of India, 1950:

Constitution does not directly have any provisions regarding the Right of Privacy but this right can be inferred from different provisions of it. Article 19(1)(d), Article 19(1)(d), Article 21 indirectly

conferred the right to privacy to every citizen of the country as Right to Life and Liberty also signifies the Right to Live with dignity and privacy is a most essential component of a dignified life.

The case of *K.S Puttaswamy v Union of India* (2017) has been a landmark judgement to grant the privacy a status of fundamental right. The case was of very high significance because earlier privacy used to be infringed by the state with actions like phone tapping, messages tapping in the name of personal internets with any scrutiny or high level regulations. This case gives the concept of privacy a new strength and leads the path for more protection to it.

Data (Protection and Privacy) Bill, 2017 & 2019:

It has certain provisions related to due diligence to be followed by intermediaries,legitimate expectations, BHIM payment system, consent criterion and online banking. It also has provision regarding the followings:

i. Obligations of Data Fiduciary/Service Provider

ii. Consent from data principles at time of data processing

iii. Creation of a Data Protection Authority

iv. Certain regulations and obligations for social media intermediaries

v. Certain exemptions in data processing for state agencies in interest of security of India, public order, sovereignty and integrity of India.

vi. Requirement of transparency and privacy design by service providers and many other relevant areas.

National Cyber Security Policy, 2013:

The policy was the outcome of the serious concerns expressed over the internet security in India. The main highlights of the policies are:

i. Facilitating the creation of secure computer environment

ii. Enabling adequate trust and confidence in electronic transactions

iii. Guiding stakeholder's actions for the protection of cyberspace.

OCED Guidelines on Protection of Privacy and Trans-border Flow of Information:

The guidelines aim to the protection of privacy and trans-border flow of personal information. The following are the highlights of the guidelines:

i. Collection of personal data with consent.

ii. Relevance of data to the subject under investigation.

iii. Specific purpose of collection.

iv. No further use without consent + legal use

v. Safeguard to prevent leakage

vi. High accountability of personal information collection information.

vii. A person right to rectification and access

viii. Collection limitation.

LAGGING OF LEGAL DOMAIN TO ENSURE PRIVACY

Though the current legislations and rules try to regulate the domain to cyberspace, still the absolute privacy seems to be a myth seeing the current scenario where such a great amount of information and data flows in online domain and the regulatory systems are lagging to provide absolute privacy protection. We here points out some of the grey areas where the legal domain is lagging:

1. There is **no specific definition of "sensitive personal information**". The definition will help in granting more privacy to it by having a different approach for it than the general information.

2. Other than some of the guidelines and conventions, **there is no minimum security standard with legal effect to which entity having control of data should comply**. The absence of any particular legislation and rules makes it easier for the entity to compromise the data.

3. These days the intermediaries like social media sites are the major platforms where there is large flow of personal data and high rate of privacy infringement like copyright

infringement, identity theft, cyber stalking, corporate espionage and many others. There is punishment for individuals doing the offence under Chapter XI of IT Act, 2000 and IPC. But there is no such minimum standard backing legally to be necessarily followed in order to protect the privacy infringement on their platforms. For the intermediaries, apart from some guidelines and few provisions of IT Act, 2000, there is **no specific legislation for the regulation and safety measures to be compulsory adopted by the intermediaries/service providers.**

4. In case of any dispute that arises because of the privacy infringement there are many dispute resolution mechanisms like Adjudicating Officer (a quasi-judicial body) under IT Act, 2000, Cyber Appellate Tribunal established under Section 58 of the IT Act, 2000.

   But the powers of Adjudicating Officers are humongous and cyber appellate tribunals and other mechanisms are practically not so much effective. The powers and punishments powers given to them are very narrow and limited and they may not be able to tackle the current issues in cyberspace.

REFORMS NEEDED TO SOLVE PRIVACY ISSUES IN CYBERSPACE

The current laws and institutions may not be sufficient to protect the gross privacy infringement that happens in cyberspace. There is need of reforms both in legislations& personal level and technology to protect the privacy. The followings are suggested reforms to improve privacy in cyberspace.

1. **User Awareness**:

   The users of cyberspace need to adopt the self-restraint on his web habits i.e. on the way he /she uses the cyberspace. There is need of exercise of due diligence on the part of users. Habits like not to use the public cyber café's for important internet transactions and sharing of sensitive personal information, preferring of high security web portals for any sensitive work by being aware about its policies and security standards, creating strong passwords in banking and important accounts to enhance security. Basically, the user at personal level needs to be aware and selective in sharing any information on the cyberspace.

   At the same time, the users of cyberspace to be aware about their rights and obligation, and legal remedies while using cyberspace.

2. **Inculcation of Cyber Ethics:**

The important reform that is needed is to develop a comprehensive code of cyber ethics which will enables to inculcate the best practices that must be adopted by the users of cyberspace while using it. It must be made a part of curriculum. It will help in creating moral and social values among the users to use the cyberspace with good behaviour and right approach which will ultimately help in minimizing the privacy infringement in cyberspace.

3. **Law Strategies :**

There is need to develop comprehensive law strategies for the cyberspace by each company, department and service providers. It will include a comprehensive compliance process, management of internal privacy, employee training, awareness, self-regulatory efforts, corporate interface with privacy awareness seminars and online dispute resolution mechanism.

4. **Intermediaries Liabilities:'**

These days most of the information flows through intermediaries like social media platforms and shopping platforms and thus most of the privacy infringement happens there or through it. Thus the intermediaries need to be more regulated and obligated in ensuring the minimum privacy infringements.

There is need of separate legislations for the intermediaries where there should be basic definitions like that of general information and personal sensitive information, minimum security standards to be necessarily adopted, identity verifications of every user that intermediaries try to shake hand with, and effective dispute resolution mechanism.

5. **Effective Dispute Resolution Mechanism:**

These days the organisation like WIPO (World Intellectual Property Organization) and ICANN (Internet Corporation for Assigned Names and Numbers) that have dispute resolution forum can cost upto $20-$100 only for registration for dispute mechanism which only big companies and rich peoples can take benefits.

The cyberspace thus needs effective dispute resolution mechanisms which would be both **cost efficient** so that it can be reached by every section of society and it also be **legally backed** so that resolved dispute can be effective on netizens.

Apart from the legal and personal level reforms, there is needed to enhance the technology for more secure cyberspace. Following are the points where technological reforms can be done:

1. **More Encryption:** The technology also has to play its part in soling privacy issues. The apps and website creators need to focus on more effective and secure encryption in data communications so that it cannot be easily breached.
2. **Anonymity of data:** The cyberspace needs more anonymity of data like clouding method in which data will not be stored in one place but keeps on changing its location which will easily to locate and to stole.
3. **Cryptography:** The current technology developers needs to focus more on cryptography methods where data is stored in an algoritmatic manner through hash function and needs a particular software with right signatures to assess it.

CONCLUSION

Thus the privacy in cyberspace has to be a priority. There are making privacy issues in cyberspace like cyber stalking, copyright infringement, spamming, identity theft, website vandalism etc. which can be of serious consequences. There are many current laws, regulations and guidelines like IT Act, Constitution, OCED guidelines, National Cyber Policy, and many others which try to tackle the privacy issues but are still lagging form the fast growing scope and working of cyberspace. The current authorities in India are trying to introduce the new legal framework like Data Protection Bill and National Cyber Policy to regulate the cyberspace in a much extensive manner.

The need of the hour is to do some big reforms like awareness programmes pan country, framing of rightful law strategies, more effective dispute resolution programmes and many other technological advancements like high encryption methods, cryptography, e-clouding of data and many others.

The time has come when the privacy have to be taken seriously as today the cyberspace has effected every individual's life so is the privacy issues in it. The cyberspace has now become an integral part

of daily life and today each and every work whether it is of government, banking, education, entertainment, security etc., is associated largely with the realm of cyberspace.