National Journal of Advanced Research
ISSN: 2455-216X; Impact Factor: RJIF 5.12
Received: 15-09-2020; Accepted: 30-09-2020; Published: 16-10-2020
www.allnationaljournal.com
Volume 6; Issue 4; 2020; Page No. 01-05

Right to privacy and unethical use of cellular data

Shubham Saini
Research B.B.A., L.L.B (HONS.) at Seedling School of Law & Governance, Jaipur National University, Jaipur, Rajasthan, India

Abstract
When it is a matter of Privacy and accountability, people always claim the former for themselves and latter for everyone else. A person's mobile number is one of the data information; a person may or may not be aware of but, is matter of his/her Right to Privacy. With the latest inclusion of Right to Privacy in Art.21 of the Indian Constitution by the Apex Court, this paper deals with a basic and petty, yet very concerning, infringement of aforesaid right i.e. Unethical use of Cellular Data by mobile number data access and personal details access (with no clue to the owner). The insurance agents, other telecom companies, jackpot/lottery agencies etc. have the easiest access into the personal details like name, address, profession, even DOB etc through one's mobile number –which actually must be private. This paper deals with the analysis of incidents (which are yet unknown as an infringement of Right to Privacy, even to the educated class of society) via imperial data collection by constructive sampling method implied in a Law College. The analysis studies two-way perspective of such infringements, the former and very common is the local perspective i.e. data access by local institutions where as other perspective is the international aspect which is quite perilous. The research also tries to find out the reasons behind it and what is TRAI's role in it. Further, paper suggests the precautions and effective measures to tackle the situation.

Keywords: Privacy, unethical, cellular data, TRAI's

Introduction: The Backdrop

Privacy may be defined as the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others [1]. Privacy incursion issues arise from data matching (the process of extensive cross checking of data from one source against another source such as tax and social security data) and personal profile extraction processes which use this data exclusively or in combination with other openly available data.

We often receive calls and messages selling products and offers. While the unknown person calling us seems to know us and our background very well, this may concern us. Our personal data hence becomes very vulnerable. Personal data may include Mobile number, Name, Address, e-mail address, occupation, your recent visits, current location etc. This data can be misused as well. Since privacy overlap with the term liberty, so the individual's right to control dissemination of information about himself is valid as it is his own personal possession. Hence the information so provided at least be protected from vulnerability, at least it can be protected from getting leaked, since it can be misused in lakh ways.

For the sake of this research, cellular data means any data which is transmitted via service providers using a cell phone. The data can be person's call logs, frequently visited websites, SMS's by banks, insurance agents, etc. along with the personal details which were provided to the telecom company during issuance of a unique mobile number.

The idea is to inculcate uniqueness of data and to bring out a different affects caused by such infringements to citizens (women in particular) and to the country as a whole.

Right to Privacy in India has been a debatable issue in recent years and it concerns the lives of many people around the world. Right to privacy is not a constitutionally but judicially recognized right. With focus on the impact of declaring privacy as a fundamental right, we are researching on the same to find out solutions for this. For which, we seek some information regarding such calls and messages with reference to your personal information.

A person's mobile number is one of the data information; a person may or may not be aware of but, is matter of his/her Right to Privacy. Privacy issues relating to personal data arise from

- insecure electronic transmissions,
- data trails and logs,
- online transactions and the
- Tracking of web pages visited.

Laws relating to data privacy and protection

Upholding data bases is not so much difficult task as maintaining its integrity, so in this esra the most fretful debate is going on to innovate a method of privacy protection. With the advancement in technological development, a transition in the standard of crimes is noticed. Nowadays most of the crimes are being done by the professionals through the easiest medium. The lust of information is acting as a catalyst in the growth of cyber-crimes.

It is the very concerning to have sufficient protection to huge databases. In the absence of any particular strict law relating to data protection, the wrongdoers are gaining expertise in their work every day.

Though, advancements have simplified our life style but it left certain irregularity in procurement of its purpose which resulted in involuntary disclosure of data. This can be scrutinized from these situations:

1. Almost once in a week, calls are received from an Unknown caller, though unknown but who is very familiar to our information. When the law students

were asked about how often they received such calls, maximum stated that once in a week. Thus, it can be observed that how much and to what extent data matching is into one's personal life.

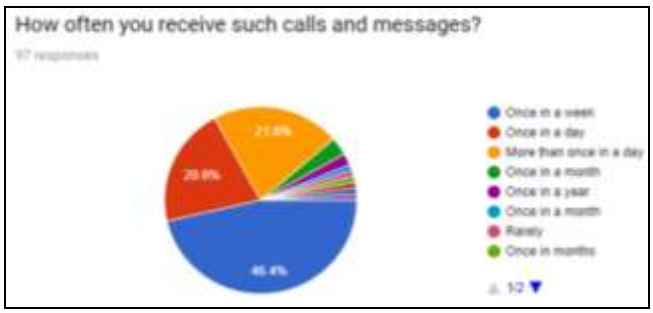

Fig 1

More than 50% of them replied that calls are received by a person who is already aware of their personal details such as name, address, websites they visit, etc.

Fig 2

This situation is concerning

2. Most of the calls are from the telecom companies and insurance and banking companies. That is very concerning because being key players in an economy and one of the most trustworthy sectors are involved in these sort of activities which ultimately leads to feeling of insecurity to the customers.

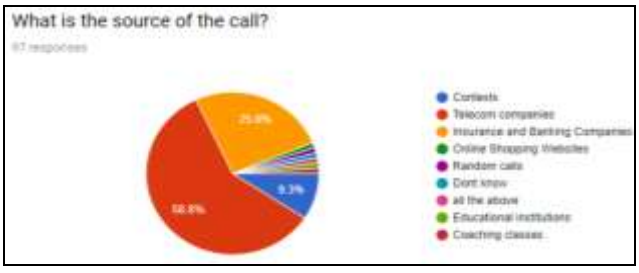

Fig 3

3. On every login to internet, there left behind an electronic trail enabling website owners and advertising companies to get access to the preference and choices of the users by tracking them. The source of information leakage remains unknown to the citizens.

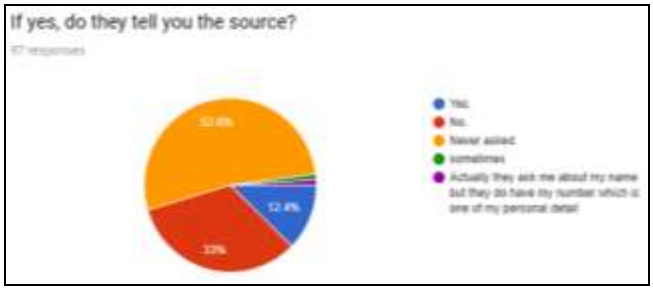

Fig 4

Thus it can be easily pointed out that how easy we are providing room to the miscreants to enhance and simplify their acts and how safe is it to avail the services of the digital world.

Data protection under Indian Law

Constitution has provided the law relating to privacy under the scope of Article 21. Its interpretation is found insufficient to provide sufficient protection to the data. The Right to Privacy is not a explicitly guaranteed as fundamental right, but the apex court has time to time interpreted it in some way as an element of fundamental rights. There have been instances in various cases decided by the apex court. The right to privacy in India has come a long way with most recent judgment in *Justice K.S Puttaswamy & Another v. Union of India*, wherein the apex court collectively held that the right to privacy is fundamental right protected under the Constitution.

In the year 2000, efforts were made by our legislature to ensure privacy issues relating to computer system under the purview of IT Act, 2000. This Act contains certain provisions which provide protection of stored data. In the year 2006, our legislature has also introduced a bill known as 'The Personal Data Protection Bill' so as to provide protection to the personal information of the person [2].

TRAI, 1997

Telecom Regulatory Authority of India Act, 1997 also does not talk about data privacy. Though, there are provisions to regulate the telecom companies but a well-established regulation for cellular data privacy is still not recognized.

Information Technology Act, 2000

- **Section 43**

This section provides protection against unauthorized access of the computer system by imposing heavy penalty up to one crore. The unauthorized downloading, extraction and copying of data are also covered under the same penalty. Clause 'c' of this section imposes penalty for unauthorized introduction of computer viruses of contaminants. Clause 'g' provides penalties for assisting the unauthorized access.

- **Section 65**

This section provides for computer source code. If anyone knowingly of intentionally conceals, destroys, alters or causes another to do as such shall have to suffer a penalty of imprisonment or fine up to 2 lakh rupees. Thus protection

has been provided against tampering of computer source documents.

- **Section 66**

Protection against hacking has been provided under this section. As per this section hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss of damage will be caused to any person and information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished. This section imposes the penalty of imprisonment of three years or fine up to two lakh rupees or both on the hacker.

- **Section 70**

This section provides protection to the data stored in the protected system. Protected systems are those computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as a protected system. Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.

- **Section 72**

This section provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both.

Though the Act covers the computer data and other related data information but the Information technology Act, 2000 also does not include "cellular data" under its protection.

Indian Penal code, 1860

It imposes punishment for the wrongs which were expected to occur till the last decade. But it failed to incorporate within itself the punishment for crimes related to data which has become the order of the day.

The personal data protection bill, 2006

This bill was introduced in the Rajya Sabha on December 8, 2006. The purpose was to provide protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act. Provisions contained in the Act are concerning to nature of data to be obtained for the specific purpose and the quantum of data to be obtained for that purpose. Data controllers have been proposed to be appointed to look upon the matters relating to violation of the proposed Act. But it doesn't include cellular data.

Though, *the Personal Data Protection Bill, 2013* again was an effort to impose right to privacy but was never passed. The Bill never recognized "cellular data" as "sensitive personal data" under definition in the aforesaid Bill [3]. Even the latest, *The Data (Privacy and Protection) Bill, 2017* which was introduced in the Lok Sabha by Sh. Baijayant Panda do not include "cellular data" and personal details under the definition of "sensitive personal data" [4].

The Scenario

- Effect on people's life and security and Problems faced by women

Integrity and personal security is one's foremost concern when it comes to privacy. a person who feels to be insecure and vulnerable.

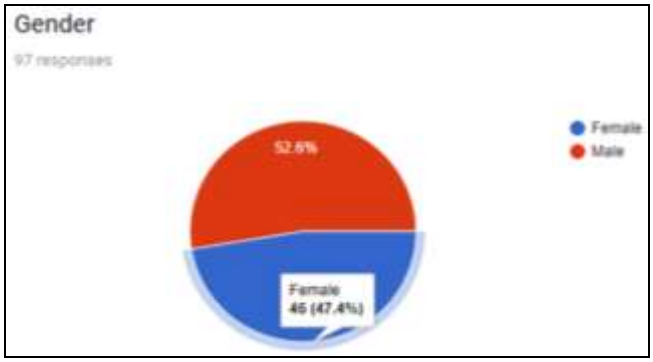

Fig 5

The survey depicts that the 47% of the responses were by females. They face many problems regarding the infringement of right to privacy, which indeed is a very sensitive matter if we are trying to empower our females. The repeated calls to women by unknown people may cause disturbances in their life even it leads to stalking, and even more heinous crimes. The mobile numbers of the women are a matter of total personal discretion of a woman to share or not. The case is same with the men. But due to lack of awareness and misuse of loopholes of the statutes, the situation becomes worse.

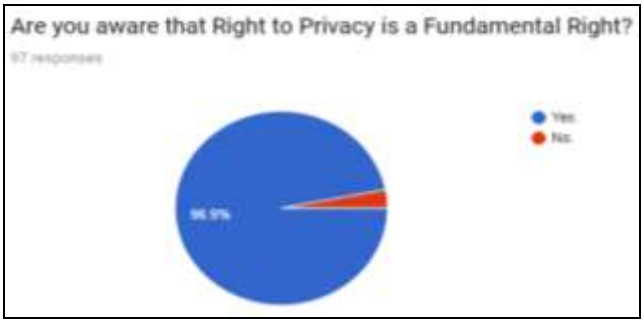

Fig 6

Though the people are aware that right to privacy is a Fundamental Right and this kind of use of "cellular data" is infringement of their right, still they are ignorant about it. The reason behind it is traced as there is no proper law or rule established against the unethical use of cellular data.

Fig 7

Also, due to the repeated calls to the unknown women or girls, their family members feel insecure and also bound and restrictions are been applied on that girl. The major concern is of the respect of the women, which is been highly exploited by the unknown people on having grudges with them.

- The International security issues

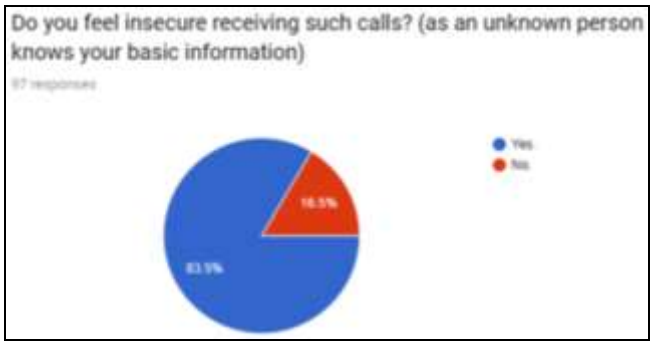

Fig 8

The survey depicts that more than three-fourth of the students said that they felt insecure, and due to the false information been spread by the international mobs through cellular data. Spreading rumors in the society leads to the internal threat to a nation. These rumors may also lead to the riots in the nation. The international calls and data could lubricate the track of public at large and to the most vital can hamper the security of people in form of physical, mental, financial, cultural, social aspects etc. The paramilitary forces, soldiers etc. and their movement can be tracked easily which can lead to sudden attacks. Financially these callers fool many people and frauds are very common in this fifth generation of computers.

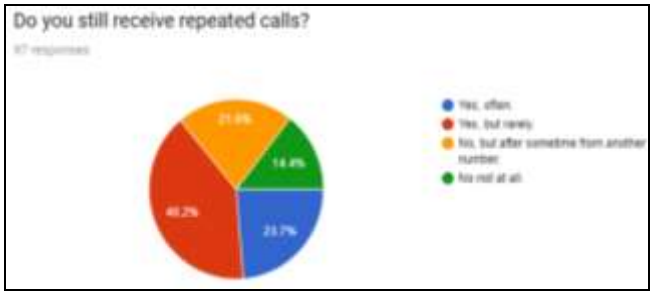

Fig 9

They also tend to disturb and distract often to trace out further information which is surveyed that repeated calls are very common.

Why it is hard to handle it out?

These days' companies are relying on contract law as a constructive means to protect their information. The corporate houses enters into several agreements with other companies, clients, agencies or partners to keep their information secured to the extent they want to secure it. Agreements such as 'non circumvention and non-disclosure' agreements, 'user license' agreements, 'referral partner' agreements etc. are entered into by them which contains confidentiality and privacy clauses and also arbitration clauses for the purpose of resolving the dispute if arises. These agreements help them in smooth running of business. BPO companies have implemented processes like BS 7799 and the ISO 17799 standards of information security management, which restrict the quantity of data that can be made available to employees of BPO and call centers.

But at the ground level the *de facto* condition is much more different. These agreements and clauses are interpreted in such a manner that the data is sold or even traded for sake of money or company secrets etc. many a times the data is leaked through insider trading and even by the analysis's who are sacked out.

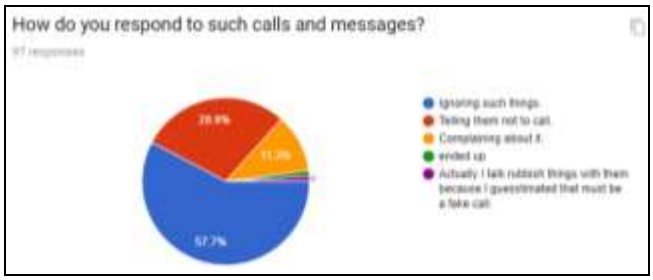

Fig 10

The survey depicts that most of the people tend to ignore such things because they don't get satisfying answers at first instance.

Tackling the situation

Without permission the leaking of data and calling unnecessarily is very disturbing and makes one worried. These should be banned completely and if needed then only the ones desiring it should be provided these calls. The state has certain responsibilities under relevant Commonwealth and State privacy legislation. Their functions include:

- handling complaints by individuals who feel their privacy rights may have been breached;
- assisting governments and private sector bodies (where applicable) comply with relevant privacy legislation;
- providing information advice to the public about their privacy rights; and
- Policy development.

To handle this particular infringement and to stop the unethical use of "cellular data" becoming an organized crime, the "cellular data" and personal details attached to it should be added as a clause under Sec. 2(s) of The Data (Privacy and Protection) Bill, 2017 and the Bill needs to be passed as soon as possible. Further till the enactment comes into force, the following compliances must be implemented:

- Intimating the called person and informing him/her regarding the basic details of the caller, as well as,

provisions of recourse in an event of breach of information (confidential or otherwise) in reference to sections 8 (1) (d), 8 (1) (j) and 13 of the Right to Information Act, 2005.

- A proper check on authorities such as TRAI because the key players in TRAI are the gigantic telecom companies who itself are indulged in these.
- The banking and insurance companies must be notified not to advertise in such manner which initiates from infringement of someone's personal right i.e. Right to Privacy.
- Mobile number protection should be increased by service providers and some immediate actions should be taken over the complaints issued by customers, people should not easy give their personal to everyone who asks for it.
- The DND(do not disturb) provision should be strengthened and implemented in a strict sense where the party who contravenes should be penalized for fraud under Indian Penal Code and every telecom network should provide this facility.
- Most of the times it is even our own fault that, as and when we download an application, we accept the terms and conditions with reading such things and we allow them to read our contacts, photos, etc,. So that should not be done through this violation has been done.

Where in a country which still is fighting against basic literacy, the population owns technology but cannot master it. That is the so reason why even the literates, intellects and as per the survey the people in the law fraternity are the victims of such infringements and most of the time they are unaware of this fact. Hence, the situation needs to be handled with care and even needs a proper recognition and attention because prevention is always better than cure.

Conclusion

On comparing the Indian law with the law of developed countries the proper requirement for the Indian law can be analyzed. Data are not of same utility and importance; it varies from one another on the basis of utility. So we require framing separate categories of data having different utility values, as the U.S have. Moreover the provisions of IT Act deal basically with extraction of data, destruction of data, etc. Companies cannot get full protection of data through that which ultimately forced them to enter into separate private contracts to keep their data secured. These contracts have the same enforceability as the general contract.

Despite the efforts being made for having a data protection law as a separate discipline, our legislature have left some lacuna in framing the bill of 2006. The bill has been drafted wholly on the structure of the UK Data Protection Act whereas today's requirement is of a comprehensive Act. Thus, it can be suggested that a compiled drafting on the basis of US laws relating to data protection would be more favorable to the today' requirement.

Being one of the most concerned topics of discussion in the modern era, legislatures are required to frame more stringent and comprehensive law for the protection of data which requires a qualitative effort rather than quantitative [5]

References

1. Westin AF. Privacy and Freedom New York: Atheneum, 1967, page 7.
2. Pankaj Kumar. Data Protection Privacy in India, http://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html.
3. Sec. 2(x), The Personal Data protection Bill, 2013.
4. Sec 2(s), the Data (Privacy and Protection) Bill, 2017.
5. Pankaj Kumar, Data Protection Privacy in India, http://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html.