International Journal of Management, IT & Engineering
Vol. 8 Issue 8, August 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Privacy in cyberspace: A Digital India perspective

Anil Kumar Bakshi*

Abstract

This paper deals with privacy in cyberspace in a developing Digital India scenario. Right to privacy of a person is under great threat due to ever growing utilisation of internet specially under Digital India program & Internet of Things whereby the internet user is under continuous electronic surveillance without his consent and without his knowledge. Recently in 2017, in Puttaswamy case, Supreme Court of India declared that right to privacy was a fundamental right . This has further compounded the problem of online privacy. Individual activities are being monitored by State as well as private parties without proper legislation for safeguarding individual's privacy. India's National Cyber Security policy of 2013 or The Information Technology Act of 2000, as amended in 2008, do not adequately address the issue of privacy in cyberspace. Govt appointed Srikrishna Committee, in 2017, is yet to submit recommendations on cyberspace data protection . A new legal framework, consisting of legislation , Special Tribunals and cyber police using remote access technique is suggested to provide possible workable solution to the present and future issues of privacy in cyberspace even in the absence of universally accepted cyber law and cyber procedure.

Keywords: -Privacy in Cyberspace, Information Technology Act, Puttaswamy judgement, Data protection

1. Introduction

The technological advancements in computers and Communication , resulting in evolution and fast expanding global cyberspace, is posing a great threat to basic human right of privacy. The existing laws, legal institutions and practices worldwide are unable to combat the menace of violation of privacy in the cyberspace due to it's unconventional organisation. Cyberspace is a virtual world created by humans by using communication technologies and computers. A common man visualises cyberspace as the imaginary place on internet where electronic messages, pictures etc are sent through computers to persons located at different places in the world and uses cyberspace accordingly. It is a global socio-techno-legal complex phenomenon which is becoming an unmanageable monster to a common man's privacy due to increasing usage of internet, e-mail, smartphone etc. Cyberspace is very unlike other tangible domains e.g. land, sea etc where physical laws can be easily applied. The cyberspace has special characteristics of being an inexpensive media which is borderless , easily accessible and provides anonymity . It also has complex legal issues which include jurisdiction, sovereignty, choice of law applicable, different social and legal standards in different countries . There are also differing viewpoints about role of state as well as role of private parties in cyberspace regarding individual's privacy. Some advocate totally free internet while some others want at least some State restrictions and both propositions directly affect the issue of privacy of an individual. Cyberspace is being increasingly used for various activities like e-commerce, e-governance, e-communication etc where an individual leaves behind his electronic whereby his privacy can be compromised.

In 1948 United Nations proclaimed UDHR (Universal Declaration of Human Rights) [1] declaring various rights of an individual including right to privacy. India's Constitution was adopted on 26-11-1949 by the constituent assembly.. Therefore , the makers of UDHR and Indian Constitution had no idea about intricacies and complexities of issues relating to cyberspace and they could not visualize about the revolutionary media of cyberspace nor could lay down the principles of law related to cyberspace. Later, in 1966, the United Nations adopted ICCPR (International Covenant of Civil and Political rights) [2] which came into force in 1976 and it's Article 17 recognised "right to privacy" .

* Advocate-on-Record , Supreme Court of India & Ph.D Scholar (Law) , Jamia Millia Islamia
r/o F-229, Vikaspuri, New Delhi -110018

In India, first public internet service was started by VSNL (Videsh Sanchar Nigam Limited) , a Govt of India enterprise , on 15 Aug 1995[3]. The number of internet and mobile phone users kept increasing after 1995. A recent Press Release note No. 04/2018 issued by the Telecom Regulatory Authority of India on 11th January 2018[4] stated that as on 30th November 2017 total wireless subscribers (GSM, CDMA, LTE) stood at 23.41 million and total broadband subscribers was 350.70 million. These figures will only increase in the future as computer and internet will be easily available in almost every home in India which will further affect the privacy of an individual .

2. Digital India programme

The Digital India programme[5] of Govt of India programme was launched by Prime Minister Narendra Modi on 1st July 2015 for the purpose of reducing paper based working in the country and instead to shift to electronically based working. It is a flagship programme of Govt of India with a vision to transform India into digitally empowered society and knowledge economy as stated by the Govt website. This programme is primarily to ensure that the Govt services are made available to citizens electronically through high speed improved internet availability and better online infrastructure. Digital infrastructure will include availability of high speed internet facility, mobile phone and bank account , internet identity, access to common service centre , and safe and secure cyberspace. Digital India covers multiple Govt ministries and Departments with overall coordination being done by Department of Electronics and information Technology , Govt of India.

High speed internet and high speed broadband connections will be available to all rural villages. Technological infrastructure will be enhanced to give digital identity through use of mobile phones and mobile phone based banking . There would be easy access to common service centres within the localities. The aim is to provide opportunity for universal digital literacy . All govt and public documents would be available digitally on cloud platform. Finally, the aim is to ensure a safe and secure cyberspace within the country. High speed internet and mobile banking would become as common as electricity. All such Govt initiatives would involve collection and use of personal data of an individual by the State as well as non-state parties. This would place an individual in a vulnerable position with a direct bearing on his privacy in the absence of suitable legislation and proper infrastructure.

3. Internet of Things (IoT)

The Internet of Things (IoT) is a recent entry to cyberspace which can be defined as interplay for software , telecommunication and electronic hardware. As per Govt of India's "IoT Policy Document" [6] IoT is a seamless connected network of embedded objects/devices , with identifiers, in which communication without any human intervention is possible using communication protocols but phones, tablets and personal computers are not included as part of IoT. Broadly speaking IoT is a network of devices that can connect to web and make normal machines as smart e.g. if a coffee making machine is connected on a smartphone then with a tap on the smartphone the coffee machine will start brewing coffee. Another example is the use of GPS capability in a car which allows the car driver to navigate through the route without a map because the GPS is connected through internet. In IoT scheme a smart refrigerator with sensors would know more about an individual's diet habits than his doctor. The smart refrigerator can tell you what is the best meal possible from the available food stuff and even what should be made for the next meal. This is all due to sensors embedded in the physical items which sense and record data which is transmitted through internet to intelligent servers where such data is collated and sifted and intelligent solution is transmitted back. A smart wrist band can identify High B.P. in a sleeping man . The wrist band would vibrate strongly to wake up the man suffering high BP , unknowingly, and simultaneously send all body vitals readings to the medical consultant where the data is analysed and urgent emergency medication is transmitted back and if required, an ambulance goes immediately to the man's house and brings him to the hospital where he is treated in time. On a much larger scale, the water supply, traffic, electricity, crowd control , movements of people etc can be monitored and controlled in a smart city through the use of IoT. However, all this also poses the problem of adversely affecting the privacy of an individual which will be exposed due to recording of so much of data about his activities and no guaranteed safeguard about protection of such data.

The Govt of India's Digital plan of 100 smart cities initially , would itself lead to a great expansion of IoT in the country. IoT involves three distinct stages : sensors for collection of data, a software application for collection and analysing data for decision making through the media of internet. The Govt feels that the key stakeholders would be the citizens , the Govt and the industry but the foreign commercial entities involved cannot be left out. The Govt vision is to develop connected and smart IoT based system for our country's Economy, Society, Environment and global needs but this vision has to be compromised due to

dependence upon foreign technology and foreign investment in India in terms of technology, manpower and finances. Under such circumstances , the govt has almost no control over foreign entities working in india for commercial gains without giving any guarantee to the citizens about safeguarding of their data. A lot of data would be collected and thereafter to be analysed for decision making through use of internet. This data is based on human activities and individual behaviour directly affecting the privacy of an individual as his data is being recorded and scanned and analysed by various third parties in India and abroad even without his knowledge or consent.

4. **Evolution of online privacy**

Privacy i.e. "to be let alone", is globally recognised as part of Human rights relating to privacy of individual's behaviour, his personal communications,, his likes and dislikesc. Indian Constitution , consisting of Fundamental rights (basic human rights) was finalised on 26-11-1949 but there was no specific mention of right to privacy. In 1954 in the case of M.P. Sharma vs Satish Chandra [7] the Supreme Court of India (8 Judges bench) held that Constitution makers had not recognised the right to privacy as a fundamental right. In 1962 the Supreme Court of India (6 Judges Bench) in the case of Kharak Singh v State of U.P [8] held that right to privacy was not a guaranteed right under the Constitution of India. The case of MP Sharma and Kharak Singh was based on the premise that relationship between various articles in part III of the Constitution were mutually exclusive. In 1994 in the case of R. Rajagopal v State of Tamil Nadu [9] the Supreme Court of India (2 Judges Bench) declared that an individual had a right to privacy. It held that the right to privacy was implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. In 1997 in the case of People's Union for Civil Liberties v Union of India [10] , the Supreme Court of India (2 Judges Bench) held that right to privacy was a part of the right to "life" and "personal liberty" under Article 21. The Supreme Court further held that telephone conversations were construed to be an important ingredient of privacy and the tapping of such conversations was held to infringe Article 21, unless permitted by law.

On 19th December 2013 the United Nations General Assembly adopted resolution [11] to the effect that the right to privacy was a human right and same that the same rights people had offline must also be protected online. It called upon the States to respect and protect the right to privacy including in the context of digital communication.

On 24-08-2017 in a landmark judgement , in case titled " Justice K S Puttaswamy (Retd) v Union of India "[12] Supreme Court of India (through 9 Judges Bench , in 6 separate but concurring judgements of 547 pages) declared the right to privacy as a Fundamental right under the Constitution of India. It declared that privacy was not only a constitutionally protected right emerging from the provision of personal liberty under Article 21 of the Constitution but it also arose from other facets of freedoms and guarantees enshrined in part III of the Indian constitution. The Supreme court overruled it's decisions in MP Sharma case and in Kharak Singh case , stated hereinabove. It was held that privacy is intrinsic to life , liberty, freedom and dignity and is therefore an inalienable natural right. The Supreme court stated that .Privacy postulated the reservation of a private space for the individual, described as the right to be let alone which enabled the individual to assert and control his human element which was inseparable from his individual personality. The Supreme court further held that thoughts and behavioural patterns which were intimate to an individual were entitled to a zone of privacy where one was free of social expectations and not judged by others. The supreme Court went on further and held that privacy was attached to the person and not to the place where it was associated and that privacy was the ultimate expression of the sanctity of the individual. Supreme Court took note of emergence of internet and it's connected Informational privacy and held that usage of internet resulted in creation of electronic tracks making personal lives open to electronic scrutiny resulting in violation of informational privacy. Supreme Court dealt upon the need for protection and confidentiality of personal data and stated that users of internet, wearable devices and social media networks did not volunteer to give their data but there was generation of vast amounts of data about individual lifestyles, choices and preferences. The Supreme court held that the balance between data regulation and individual privacy was a complex issues requiring delicate balances to be drawn between the legitimate concerns of the State like national security, economic welfare of poor people but the State had also to consider protection of individual's privacy online and the data collected by the State had to be utilised for legitimate purposes. This declaration has brought out new obligations for the State to protect and support it's citizens in cyberspace specially against electronic surveillance and to provide for comprehensive legal framework and set up.

With the evolution of cyberspace and increasing usage of internet for various activities there is grave threat to protection of privacy of an individual in cyberspace. Internet privacy, also commonly referred to as online

privacy, is the privacy and protection of personal data of an individual due to usage of internet by him . The term "data" is defined in section 2(1)(o) of The Information Technology Act, 2000 [13] as representation of facts in a formalised manner . Data becomes information after the collection and analysis of facts . Data are simply facts or figures e.g. history of temperature readings all over the world for the last 50 years is data but when this data is organised and analysed to find that global temperature is rising then that becomes information. The data of a person's activities on internet are collected, processed and interpreted so as to make them meaningful and usable by interested third parties. Internet privacy can be understood as privacy rights online with respect to individual's data . A user on internet is under constant tracking and surveillance by state and private agencies who are collecting his data without his consent and without his knowledge.

Privacy in cyberspace is totally different from the privacy in physical world. One may be physically isolated and working in a total physical private atmosphere but the moment one enters the cyberspace, through internet or other means, one's activities are under constant surveillance and being monitored every second , by unknown third parties, without his knowledge or consent. Thus, privacy in cyberspace assumes another dimension alongwith various legal challenges. The virtual world is in reality a public place with no privacy. The internet has become all pervasive as individuals spend more and more time online each day of their lives. Internet privacy and anonymity are of great importance to individual users specially as e-commerce continues to expand globally. The nature of online privacy is very dynamic and therefore online privacy issues and legal challenges change very rapidly. Seemingly harmless data such as websites visited can be analysed to identify individuals and learn about his personal behaviour and his personal information. Social media sites, online transactions, mobile phones registering location data, becomes information through each use of internet . In all cases individual does not know as to who all are accessing his such personal information . Further, there is absolutely no control over usage and handling of such personal information. The status of information on social media cannot be strictly demarcated into private and public spheres. The borderless information over the internet is subjected to various jurisdictions. An Indian using Gmail will be subject to laws of U.S.A. since Gmail's headquarter and servers are in U.S.A. The Govt of U.S.A can access and use Indian's data without any permission or consent from Indian Govt or the individual. Moreover, an Indian has no control whatsoever if his data is passed on to private parties in U.S.A. Presently, there are no data protection laws or in India. The Information Technology Act, 2000, as amended in 2008 , does not address the entire issues of online privacy as internet usage creates privacy risks of being exposed to phishing, spyware and malware.

5. Present legal framework and policies

The issue of privacy in cyberspace was very scantily covered under the provisions of The Information Technology Act, 2000 which was enacted to primarily facilitate e-commerce and Electronic Governance. The statement of objects and reasons mentioned that there was a need for bringing in suitable amendments to facilitate e-commerce. It further stated that there was an effort to prevent misuse over transactions in electronic medium and created civil and criminal liabilities for contravention of provisions of the Information Technology Act. Section 72 contained provisions for breach of confidentiality and privacy. Section 79 contained provisions for liabilities of intermediaries only under certain circumstances. Civil courts are barred from adjudicating on such subject as Adjudication officer has been appointed under the Information technology Act. Thus, the online privacy issue was not properly addressed .

The Information Technology Amendment Act, 2008 was passed (notified in 2009) to keep pace with the changing online scenario with technological advancements. The amendments included new provisions with respect to data protection and privacy obligations, Liability of Intermediaries, Govt interception & Monitoring, and the Enforcement Institutional framework. The new Section 43A lays down that if a body corporate dealing with any sensitive personal data is negligent in ensuring reasonable security practices and procedures which causes wrongful loss or gain to any person then such body corporate would be liable to pay damages to the person adversely affected. The new Section 72A lays down that any person , including an intermediary, who has secured access to any personal information , discloses such information to an unauthorised person in an unauthorised manner then such person would be punished with imprisonment for three years or fine upto Rs Five Lakhs or both . The new Section 66E provides for punishment for violation of privacy of private areas of a person , upto three years of imprisonment or with fine upto Rs Two Lakhs or both. The new section 69A empowers the Govt to issue directions for blocking public access to any information through any computer resource. If an intermediary fails to comply with Govt directions , then such intermediary can be subjected to imprisonment for seven years and fine. The new section 69B empowers the Govt to authorise monitoring and collection of traffic data or information for the purpose of cyber security. If an intermediary fails to comply with Govt orders , then such intermediary can be subjected to imprisonment for three years and fine. The new section 70A empowers the Govt to set up the National

Nodal agency in respect of Critical Information Infrastructure Protection . Such nodal agency would be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure. The new section 70B empowers the Govt to set up the Indian Computer Emergency Response Team (ICERT) to serve as a nodal agency for performing the functions related to cyber security. Under the amended Section 48 the Central Govt shall set up one or more Cyber Appellate Tribunals for adjudicating upon appeals against the orders of Controller or Adjudicating Officer.

In line with improved awareness about cyberspace activities and privacy concerns Ministry of Electronics & Information Technology , Govt of India framed certain Rules some of which are as under :

(i) The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009[14] whereby Secretary level officer at Union or State level is the competent authority to order interception , monitoring etc and such directions be forwarded within seven days to Review committee which will meet at least once in two months

(ii) The Information Technology (Procedure and Safeguards for Blocking Access of Information by Public) Rules, 2009 [15] whereby designated officer is not below rank of Jt Secretary of Govt of India for ordering blocking of any website , any person can send request to Nodal officer who will send it to Designated officer .

(iii) The Information Technology (Procedure and Safeguard for Monitoring and Collecting of Traffic Data or Information) Rules, 2009 [16] whereby competent authority is Secretary to Govt of India in Department of Information Technology.

(iv) The Information Technology (Reasonable Security Practices and procedures and Sensitive Personal Data or Information) Rules, 2011[17] wherein sensitive personal data or information is defined as consisting of password, financial information, physical or mental health condition, sexual orientation, medical records and history,, biometric information.

(v) The Information Technology (Guidelines for Cyber Café) Rules, 2011[18] whereby cyber café is to be registered with unique registration number and user's identity to be established and record kept for one year; all computers to be equipped with commercially available safety or filtering software.

(vi) The Information Technology (Intermediaries Guidelines) Rules, 2011[19] for due diligence to be observed by intermediaries.

On 16th October 2012 , Planning Commission, Govt of India constituted Group of Experts, under the chairmanship of Justice AP Shah, Former Chief Justice , Delhi High Court, vide it's report of ninety one pages [20] proposed a framework for the protection of privacy concerns to serve as a conceptual foundation for legislation protecting privacy. This report is yet to be fully implemented.

Govt of India , Ministry of Electronics and Information Technology (MeitY) , released it's National Cyber Security Policy -2013 [21] which was a nine pages document laying down vision for cyber security with a set of sustained & co-ordinated strategies for implementation. The policy provides an overview of it takes to effectively protect information, information systems & networks and also gives an insight into the Govt's approach and strategy for protection of cyberspace in the country. This policy is yet to be fully implemented through Legislative and Executive actions.

Recently , in 2017, the Govt has initiated the process of reviewing the entire area of data protection by setting up Srikrishna committee chaired by Justice B N Srikrishna, former Judge of the Supreme Court of India and asked the committee to study various issues relating to data protection in India and to give its recommendations. In Nov 2017 the committee released a white paper [22] and called upon stakeholders to discuss and debate various issues to ensure growth of digital economy while keeping personal data of citizens secure and protected. The paper proposed a high powered statutory authority with regulatory capacities.

6. Suggestions / Recommendations

Supreme court of India has declared that the right to privacy, including privacy in cyberspace, is a fundamental right thereby placing the state under an obligation to ensure safe and secure cyberspace where an individual's privacy could be protected . However, such a task is extremely difficult to achieve without technological knowhow and without co-operation at global level, through United Nations or otherwise. Thus, there is need for international acceptable legal frameworks, policies and procedures relating to cyberspace . The State ,, within it's borders , has to make appropriate legislation and to implement it with suitable executive actions to be able to provide at least limited workable safe and secure cyberspace to it's citizens. State should be technically self sufficient so that it can have it's own servers and does not have to depend upon foreign servers and foreign service providers. With the growing involvement of it's citizens in cyberspace due to Digital India Programme and Internet of Things there is urgent need for suitable legislation covering totality of activities in cyberspace which could be named Law of Cyber just like Law of Sea , covering civil and criminal aspects and procedural as well as substantive aspects . There should be special adjudicating tribunals , located next to police stations, consisting of legal experts / Judges and technical experts to be able to provide suitable online protection to citizens throughout day and night. There is requirement of proper adjudicating authorities / institutions / cyber tribunals set up to be able to provide real time online privacy protection service to citizens even in physical remote areas which are otherwise not technically remote areas. There should be mandatory registration of every internet user just like passport registration so that Govt can take suitable measures for protection of individual's online privacy . There should be voluntary permissible cyber policing by the Govt. and non-Govt agencies by special cyber police officers through remote access technology . The private stakeholders , including the commercial entities and private individuals will have to be involved and given certain surveillance, policing and adjudication powers. Every user of internet should be well versed with safety precautions and preventive measures so as to able to reduce the chances of violation of his online privacy by unknown persons.

7. Conclusion

There is great effort to empower India digitally but this also carries enhanced online risks as internet connected facilities can be made to crash by anti social elements against which there are no suitable protections available .Digital India programme and Internet of things will result in increasing dependence on the use of cyberspace , through internet or other devices, which will further expose an individual's life to violation of online privacy. Thus , online privacy would become even more serious an issue in the coming times. A safe and secure cyberspace is desirable based upon fine balance between state responsibilities of national security , economic and social concerns and online privacy of the citizen. However, such secure cyberspace will be difficult to achieve without international co-operation and responsive State and alert citizens.

References

[1] www.un.org/en/universal-declaration-human-rights/
[2] https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[3] https://www.news18.com/news/tech/20-years-of-internet-in-india-on-august-1995-public-internet-access-was-launched-in-india-1039859.html
[4] https://www.trai.gov.in/sites/default/files/Press_ReleaseNo4_Eng_11012018_0.pdf
[5] www.digitalindia.gov.in
[6] Meity.gov.in/content/internet-things
[7] AIR 1954 SC 300
[8] AIR 1963 SC 1295
[9] (1994) 6 SCC 632
[10] (1997) 1 SCC 301
[11] https://ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx
[12] (2017)10 SCALE 1
[13] meity.gov.in/content/information-technology-act-2000
[14] ibid
[15]ibid
[16] ibid

[17] ibid
[18] ibid
[19] ibid
[20] planningcommission.nic.in/reports/genrep/rep_privacy.pdf
[21] meity.gov.in/content/national-cyber-security-policy-2013-1
[22] meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf