Indian Approach to Privacy in Cyberspace

M. Tariq Banday
Department of Electronics & Inst. Technology
University of Kashmir
Srinagar, India
e-mail: sgrmtb@yahoo.com

Farooq Ahmad Mir
Department of Law
University of Kashmir
Srinagar, India
e-mail: far_lwtr@rediffmail.com

***Abstract*—Privacy as a right has genesis in the technology of printing and photography. This technology was viewed as impinging confidentiality of individual. Privacy right has been expanded over the years to enfold its other aspects and has been made actionable against an individual under law of Torts and redress-able against State under Constitutional Law for violating autonomy of an individual. Digital Technology has privacy issues. These issues cannot be addressed by applying traditional principles. Furthermore, Information Technology Act (IT Act) in India has been amended in the year 2008 which has given enormous powers to the Centre and State Governments to invade privacy. This paper makes an attempt to raise privacy issues pertinent to cyberspace, examines Indian judicial approach to constitutional right to privacy and evaluates technological approach to privacy.**

Keywords—Privacy; Interception; Monitoring; Privacy & Security; IT ACT 2008; Judicial Approach to Privacy

I. PRIVACY ISSUES IN CYBERSPACE

Development of privacy jurisprudence is intimately associated with technological developments much before Internet came on the horizon. Its seeds were sown at the end of the nineteenth century, following the publication of Warren and Brandies article, the right to privacy [1]. This article was prompted by the technological innovations of print media (newspapers) and the portable camera (photographs) which were thought to have potential to invade personal privacy. J. Thomas Cooly in a celebrated case of *Olmstead v. United State*[1] crystalized this doctrine by declaring that every individual has a right to be let alone. Invasion of privacy means an unjustified exploitation of one's personality or intrusion into one's personal activity, actionable under tort law and sometimes under constitutional law. Initially this right was confined to what later became its essential but not exclusive component, the right to protect the confidentiality of one's private sphere against public or private interference. Soon this right was expanded to en-cover four distinct torts that may possibly arise in case of breach of privacy a) intrusion upon a person's solitude or seclusion or into his affairs, b) public disclosure of embarrassing facts of a person's private life, c) publicity which places an individual in false light in public eyes, and d) appropriation to a person's advantage of another's name or likeness [2].

The concept and the right of privacy have undergone a significant evolution, due to the Socio-economic developments and, much more, due to the introduction of the information Communications Technologies (ICT) into daily life [3]. Equally the amount of data collected by cameras and biometric systems through the use of automated devices and their intelligent use in order to provide personalized services, clearly, gives rise to privacy problems [4].

Digital technology has changed form as well as the nature of the privacy right. In recent years, the World Wide Web, particularly Web 2.0, has raised challenges for privacy, as it fuses together voices, text, pictures, recording and retrieval technologies, and a larger capacity for the incidental gathering of details of people's private lives [5]. It involves more voices than previous Internet technologies. Blogs, wikis, online social networks, and massively multiplayer online games allow more people to communicate and interact more than ever before, about their own self or about their surroundings. This raises a plethora of privacy concerns differing in content and ambit from that which was traditionally known. Earlier Internet privacy concerns related predominantly to the aggregation of personal information to create large-scale, text-based digital dossiers about individuals [6].

Interactive Web 2.0 technology has led to an increasing tendency for people to publish texts, photographs, videos, locations, tags and preferences online, thereby placing a good deal of private life on record [7]. With more voices online, there is a wider scope for privacy invasion. With more recording technologies readily at hand such as cell phone cameras and text messaging services like Twitter—there is a wider scope for incidental gathering of details of people's private lives that can be uploaded and disseminated globally at the mouse click.

These developments have blurred the boundaries between the public and private spheres or at least are becoming more difficult to discern. Thus, any privacy laws premised on conceptions of a "reasonable expectation of privacy" are becoming more difficult to apply [8]. Facebook founder Mark Zuckerberg has argued that social changes mean that privacy is no longer a norm [9]. The privacy issues cropped up by the technology cannot be resolved by

[1] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

 ISBN: 978-1-61208-182-3

applying traditional approach to right to privacy. This is the reason that the privacy jurisprudence was revisited in the light of the developments that took place by the introduction of Internet. The right to privacy is now loaded with fresh contents and it is contended that its breach would include: a) information collection, consists of surveillance and interrogation, b) information processing, involves taking the information gathered and making sense out of the raw facts for any probable use which can be further classified into aggregation, identification, insecurity, secondary use and exclusion, c) information dissemination, concerned with the dissemination of the information and it consists of the breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion, and d) invasion, concerning invasive acts that disturb one's tranquility or solitude without concerning information [10].

In digital age, breach of privacy cannot be properly addressed if it is circumscribed by 'the right to leave alone.' Privacy is about knowing 'what data is being collected' and 'what is happening to it', having choices about how it is collected and used, and being confident that it is secure.[2]

The importance of marketable information has been so profound that it is argued that privacy as a fundamental concept should extend its reach to 'information privacy' for online transactions and personally identifiable information [11] that would include an individual's claim to control the terms under which 'personal information' is acquired, disclosed, and used.[3]

II. INDIAN CONSTITUTIONAL APPROACH TO PRIVACY

The right to privacy as a fundamental right was accorded recognition in India much before the Independence of India and adoption of the Indian Constitution. The Allahabad High Court in *Nihal Chand* v.*Bhawan Dei*[4] made the following pertinent observation:

'The right to privacy based on social custom is different from a right to privacy based on natural modesty and human morality, the latter is not confined to any class, creed, colour or race and it is birth right of any human being and is sacred and should be observed.'

The right to privacy as a fundamental right has not been expressly mentioned in the Indian Constitution. The courts in India have stretched Article 21[5] to encompass right to privacy as a fundamental right by holding that right to life means a dignified life. This right to privacy like other fundamental rights is not an absolute right but admits reasonable restriction.

The Supreme Court of India has, immediately after the adoption of the Constitution, laid down foundation for privacy jurisprudence in *M P Sharma* v. *Satish Chandra*[6]. It was held that a power of search and seizure is in any system of State for the protection of social security and the power is necessarily regulated by law. This positive approach was carried further in *Kharak Singh* v. *State of UP*[7] by J. Subba Rao, the architect of modern privacy Jurisprudence. The Apex court found seeds of privacy jurisprudence in Article 21 and held that this Article is comprehensive enough to include right to privacy. The pertinent observation, valid for all times to come, is that a person's house, where he lives with his family is his "castle" and nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy. This right was further fortified in *Gobind* v. *State of MP* [8] by accepting limited recognition in Articles 19(a)(d) in addition to Article 21. While expanding horizons of privacy jurisprudence, the Supreme Court held that right to liberty, right to move freely throughout the territory of India and the freedom of speech taken together create an independent right to privacy. In the words of Justice Mathews, the fundamental rights explicitly guaranteed to a citizen have penumbral zones and the right to privacy is itself a fundamental right. The apex court formulated the following principles to govern the right to privacy:

a) Privacy – dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior,
b) If the court does not find that a claimed right is entitled to protection as a fundamental right, a law infringing it must satisfy the compelling state interest test,
c) Privacy primarily concerns the individual. It therefore relates to and overlaps with the concept of liberty,
d) The most serious advocates of privacy must confess that there are serious problems of defining the essence and scope of the right. Privacy interest in autonomy must also be placed in the context of other right s and values, and
e) Any right to privacy must encompass and protect the personal intimacy of the home, the family, marriage, motherhood, procreation and child rearing.

Malak Singh v. *State of Punjab*[9] represents an extended reach of privacy jurisprudence. The apex court held that a surveillance of the subject by the state is intrusive and an encroachment upon his right to privacy. This approach was taken to new heights by the Indian Courts in a number of cases[10].

[2] Testimony of Mr. Erich Anderson, Deputy General Counsel of Microsoft Corporation, *The State of Online Consumer Privacy, Hearing before S. Comm. on Commerce, Science, and Transportation*, 112th Cong., (2011) (hereinafter Microsoft testimony)

[3] U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Commentary 2 (1995)

[4] AIR 1935 All. 1002

[5] Article 21, "Protection of Life and Personal Liberty" No person shall be deprived of his life or personal liberty except according to procedure established by law.

[6] AIR 1954 SC 300

[7] AIR 1963 SC 1295

[8] (1957) 2 SCC 148

[9] (1981)1 SCC 301

[10] See for instance, *PUCL* v. *Union of India*. AIR 1991 SC 207; *State of Maharashtra* v.*Madhukar Narayan Mordikar,* AIR 1999 SC 495; *Mr.X* v. *Z Hospital*, (1998) 8S CC 996; *R. Rajagopal* v. *State of Tamil Nadu,* AIR 1995 SC 264; *District Registrar and Collector* v. *Canara Bank* AIR 2005 SC 186

On technology front, the apex court found an opportunity more than once to pronounce that the privacy right exists even when the technology is used to circumvent this right. In *R.M. Malkani* v. *State of Maharashtra*[11] the apex court held that the telephonic conversation of an innocent person would be protected by the courts against wrongful or high handed interference by tapping of the conversation by the police. A more elaborative approach was adopted by the apex court in *Peoples Union for Civil Liberties* v. *Union of India*[12]. It was held that the telephonic tapping, a form of technological eavesdropping, infringes the right to privacy. Justice Kuldeep Singh laid down that the telephone taping which amounts to intrusion into privacy can take place only in the gravest of grave situation when national security is endangered and not otherwise. In usual or normal circumstance, there should not be any phone tapping and the person should not be under surveillance because he has right to privacy, which is a part of the right to life and is recognized by the constitution of India.

III. LIMITS OF PRIVACY RIGHT

The courts in India have maintained that like other fundamental rights, the right to privacy is not absolute. This right cannot be claimed where the information sought to be published or disseminated is already in public domain[13] or there is reasonable excuse available. This right to privacy is available only against the State and not against any private individual[14]. In a more recent case of *State of Maharashtra* v. *Bharat Shanti Lal Shah*[15], the apex court observed that "interception of conversation though constitutes an invasion of an Individual's right of privacy but the said right can be curtailed in accordance with procedure validly established by law. Thus, what the court is required to see is that the procedure itself must be fair, just and reasonable and non-arbitrary, fanciful or oppressive.

IV. JUDICIAL APPROACH TO PRIVACY IN CYBERSPACE

Indian judiciary has not yet found an opportunity to deliberate on the privacy issues associated with cyberspace but there are instances in transnational jurisdictions where courts have authoritatively invoked privacy right in cyberspace. In America, the Supreme Court in *Whalen v. Roe*, [16] recognized an implicit constitutional right of informational privacy. A New York law empowered to create a centralized state computer file of the names and addresses of all persons who obtained medicines containing narcotics pursuant to a doctor's prescription. The Court upheld the validity of the law, nevertheless, it held that this gathering of information impinges upon two interests. The first was an individual interest in avoiding disclosure of personal matters; the other, the interest in independence in making certain kinds of important decisions. These two interests rest on the substantive due process protections found in the Fifth and Fourteenth Amendments.

The courts in America have in a good number of cases upheld in different contexts citizen's right to privacy in cyberspace. In *US v. Ziegler*, [17] an employee had accessed child pornography websites from his workplace. His employer noticed his activities, made copies of the hard drive, and gave the FBI the employee's computer. At his criminal trial, Ziegler filed a motion to suppress the evidence because he argued that the government violated his Fourth Amendment rights.

The Ninth Circuit allowed the lower court to admit the child pornography as evidence. After reviewing relevant Supreme Court opinions on a reasonable expectation of privacy, the Court acknowledged that Ziegler had a reasonable expectation of privacy at his office and on his computer. That Court also found that his employer could consent to a government search of the computer and that, therefore, the search did not violate Ziegler's Fourth Amendment rights.

The New Jersey Supreme Court held in *State v. Reid* [18] that computer users have a reasonable expectation of privacy concerning the personal information they give to their ISPs. This case also serves as an illustration of how case law on privacy regarding workplace computers is still evolving.

In *Robbins v. Lower Merion School District* [19] (U.S. Eastern District of Pennsylvania 2010), the federal trial court issued an injunction against the school district after plaintiffs charged two suburban Philadelphia high schools violated the privacy of students and others when they secretly spied on students by surreptitiously and remotely activating webcams embedded in school-issued laptops the students were using at home. The schools admitted to secretly snapping over 66,000 web-shots and screenshots, including webcam shots of students in their bedrooms.

In a recent decision [20], the Court reconfirmed its recognition of a constitutional right to information privacy. The contract workers of National Aeronautics and Space Administration (NASA) contended they are required to answer questions about their drug treatment and are asked their references whether they have any reason to question the

[11] AIR 1973 SC 157.

[12] AIR (1997) 1 SCC 301.

[13] In *Petronet LNG Ltd.* v. *Indian Petro Group*, (2009) 95 S.C.L. 207 (Delhi) (India) the case concerned an application for an injunction against the defendants from publishing information which the plaintiff alleged was confidential. The plaintiff alleged that the defendant breached its privacy by accessing as well as disseminating information. The court held that the information was freely available in public and hence the defendant was not in breach of the plaintiff's right to privacy; Similarly in *Rajinder* Jaina v. *Central Information Commission*, 164 (2009) D.L.T. 153 the case concerned a writ petition about the disclosure of information under the Right to Information Act, 2005 wherein the petitioner challenged the disclosure on grounds of infringement of the right to privacy. The court held that the information already existed in the public domain and no claims as to privacy could be made.

[14] *See*, *Khushwant Singh* v. *Maneka Gandhi*, A.I.R. 2002 Del. 58; Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006 (High Court of Delhi, 12th October 2007) (India). The court noted that the enforcement of the right to privacy under the Indian constitutional scheme can only be made against state instrumentalities and not against private persons.

[15] (2008) 13 S.C.C. 5 (India) (*Per* K. G. Balakrishnan, C. J. et al.).

[16] 429 U.S. 589 (1977)

[17] F.3d 1077 (9th Cir. Jan. 30, 2007, No. 05-30177)

[18] lawlibrary.rutgers.edu. Retrieved 2011-11-25

[19] Doug Stanglin (February 18, 2010). "School district accused of spying on kids via laptop webcams". USA Today. Retrieved February 19, 2010.

[20] 131 S. Ct. 746 (2011)

individual's honesty or trustworthiness. NASA thus violated their privacy rights under the U.S. Constitution. The court rejected this contention 8-0. The court recognized individual's right to informational privacy but also recognized Government's legitimate interest and held that the Government is not precluded from taking reasonable steps to serve its legitimate interests for public good.

V. TECHNOLOGICAL APPROACH TO PRIVACY IN INDIA

Recent measures for the fight against terrorism and organized crime do stipulate serious interference with common human rights - particularly in form of monitoring and interception of information of individuals in India. There has been a constant debate about the supremacy of individual's fundamental right and the state's sovereign power to maintain security and in turn integrity of the country. This debate has sharpened after 9/11 in America [12] and 26/11 in India. The Governments have given legal mandate to the use of technology for monitoring and surveillance. The Indian Government framed Rules in April, 2011 asking Internet service providers to delete information posted on websites that officials or private citizens deemed disparaging or harassing. The Government also plans to set up its own unit to monitor information posted on websites and social media sites. (Govt. faceoff brewing with Facebook, others, Times of India, 5th December, 2011)

The growing interest in the new surveillance technology is precisely due to the fact that these technologies have enormously increased government's capacity to develop record keeping instruments and refined instruments of control that often impinges upon the privacy and other associated rights. This has resulted in the enactment of Data Protection laws in many countries that are based on the premise that autonomous fundamental right have to be preserved in all levels that involve personal data processing for private or public aims but there may be situations in which states can deny right to privacy in public good and counter terrorism is one of them for the aims of which security agencies can investigate and check persons or personal belongings also with new technological systems. However, counter terrorism, in no case can legalize all the interferences in the private spheres of individuals. There has to be reasonable nexus between the means and the objective to be achieved [13]. After all, a decent treatment of people in society represents a core value of data protection, and implies that people know when and for what purpose their data are collected. This may, however, prove a high degree of privacy protection especially in the present Indian context as is evinced by the following provision of the IT Act.

A. Power to Decrypt Information

Prior to Amendment Act, 2008, the Controller of the Certifying Authorities had power to decrypt any information in the interest of sovereignty, security, and integrity of the country. This power has been taken from the Controller and is given to the Central or State Government or any of its officers especially authorized by the Central or State Government as the case may be. From mere power of the Controller to decrypt information, the Central Government or the State Government has enormous powers which include:

a) Power to intercept, monitor, or decrypt any information, and
b) Power to monitor and collect traffic data or information.

B. Power to Intercept, monitor or decrypt any Information

The Central or State Government or any of its officers who has been specially authorized by the Central or State Government as the case may be, may direct any agency of the appropriate Government to intercept or monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource[21]. The term 'decryption' means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof[22].

The word 'intercept' with its grammatical variation and cognate expressions means aural or other acquisition of the contents of any information through the use of any means, including an interception device, so as to make some or all of the contents of information available to a person other than the sender or recipient or intended recipient of that communication, and includes:

a) Monitoring of any such information by means of any monitoring device,
b) Viewing, examination or inspection of the contents of any direct or indirect information, and
c) Diversion of any direct or indirect information from its intended destination to any other destination.[23]

The word 'monitor' with its grammatical variations and cognate expressions, includes to view or to inspect or listen to or record information by means of a monitoring device[24].

The above power is not limitless. It can be exercised only when the authority empowered is satisfied that it is necessary or expedient so to do, in the interest of:

a) Sovereignty of India, or
b) Integrity of India, or
c) Defense of India, or
d) Security of the State, or
e) Friendly relations with the foreign States, or Public order, or
f) For preventing incitement to the commission of any cognizable offence relating to above, or
g) For investigation of any offence.

Before any order is issued under this provision, the competent authority has to record reasons in writing for making such order. The competent authority for this purpose means:

a) The Secretary in the Ministry of Home Affairs in case of the Central Government, or

[21] Section 69 of the IT Act
[22] Rule 2 (f) of the IT Act (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009
[23] Rule 2 (i) (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009
[24] Rule 2 (o) (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009

 ISBN: 978-1-61208-182-3

b) The Secretary in charge of the Home Department, in case of the State Government or the Union territory as the case may be.[25] The competent authority may call any subscriber or intermediary or any person in-charge of the computer resource that shall extend all facilities and technical assistance to:

- Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information, or
- Intercept, monitor, or decrypt the information, as the case may be, or
- Provide information stored in computer resource.

The subscriber or intermediary or any person who fails to assist the competent authority shall be punished with imprisonment for a term which may extend to seven years and shall be also liable to fine. The term intermediary with respect to any particular electronic record means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.[26]

The above provision finds parallel in Section 5(2) of the Telegraph Act that has been framed in pursuance to the Supreme Court pronouncement in *PUCL v. Union of India*[27]. These rules provide when a) public emergency, or b) public safety situation exists, then an order may be made to issue directions for interception. These rules effectively authorize to issue directions for the interception of messages. A balancing measure to safeguard against a blanket violation of privacy has been provided. The section itself provides for several safeguards that include recording of reasons for taking any of these steps. These measures cannot be taken unless it is shown that such step is necessary or expedient in the interest of a) sovereignty and integrity of India, b) the security of the state, c) friendly relations with foreign states, d) public order, and e) incitement to the commission of an offence. There is no direct case decided by any court in India on the above issue. However, recently the United States court of Appeals for the district of Columbia Circuit in Appellee vs. Lawrence Maynard[28] had an opportunity to decide effect of use of GPS on privacy right of an individual. The court observed that the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave. A search conducted without a warrant is per se unreasonable under the fourth amendment subject only to a few specifically established and well delineated exceptions. The court gave go ahead to the use of technology for surveillance purpose for security reasons subject to certain safeguards.

[25] Rule 2 (d) of the IT Act (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009
[26] Section 2 (w) of the IT Act
[27] Supra note 12
[28] No. 08-0330 decided on August 6, 2010

C. Procedure for Interception, Monitoring, or Decryption of any information

The circumstances warranting interception, monitoring and decryption of information can be classified into three categories, namely: a) Normal, b) unavoidable, and c) Emergency[29]. The interception, monitoring, or decryption of any information can be carried out in normal circumstances only by an order issued by the competent authority. No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource, except by an order issued by the competent authority. The interception, monitoring, or decryption of any information can be carried out in unavoidable circumstances by an officer not below the rank of the joint secretary to the Government of India, provided that he has been duly authorized by the competent authority.

Emergency cases have been subdivided into two categories: a) Locational, and, b) operational. The interception, monitoring, or decryption of any information may be required in a remote area but obtaining of prior directions for such interception or monitoring or decryption of information is not feasible. Or where obtaining of prior directions for interception or monitoring or decryption of any information generated, transmitted, received or store in any computer resource, for operational reasons, is not feasible.

In the emergency cases, resulted by locational or operational reasons, the interception, monitoring, or decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency at the central level and the officer and the officer authorized in this behalf not below the rank of Inspector General of Police or an officer of equivalent rank at the State or Union territory level.

The officer, who has permitted the interception, monitoring, or decryption of any information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception, monitoring, or decryption within three days. The concerned officer must obtain the approval of the competent authority within the period of seven working days. If the approval of the competent authority has not been obtained within the stipulated time of seven working days, such interception, monitoring, or decryption shall cease and the information shall not be intercepted, monitored or decrypted thereafter without the prior approval of the competent authority.

It is quite possible that the State Government or Union Territory administration may require interception, monitoring, or decryption of any information beyond its territorial Jurisdiction. The Secretary in-charge of the Home Department in that State or Union Territory, as the case may be, shall make a request to the secretary in the Ministry of Home Affairs, Government of India for issuing direction to

[29] Rule 3 of the IT Act (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009

 ISBN: 978-1-61208-182-3

the appropriate authority for such interception, monitoring, or decryption of information.

The competent authority shall consider possibility of acquiring the necessary information by other means and the direction shall be issued only when it is not possible to acquire the information by any other reasonable means.

Every direction shall specify the name and designation of the officer of the authorized agency to whom the intercepted, monitored or decrypted information shall be subject to the provisions of the IT Act. The direction for interception or monitoring or decryption shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty days.

The above provisions have been incorporated by the Amendment Act, 2008 and attempt to remove the limitations of the original Act by making IT Act a complete code for Internet behavior. This provision, like Section 69 has roots in the ratio of *PUCL v. Union of India*[30] wherein the court has held that the direction may only be issued when it is warranted by a) public emergency; or b) public safety. These limitations are based on Section 5(2) of the Telegraph Act. The direction must contain reasons for taking such measures. It also contains the requirement of recording for which the prescribed procedure under section 69(2) has to be followed.

VI. CRIMINAL LIABILITY FOR VIOLATION OF PRIVACY

The IT (Amendment) Act has carved out a new provision which makes capturing of an "image of the private area of a person", under circumstances violating the privacy of the person, punishable. The circumstances violating the privacy of a person are when such person has a reasonable expectation that a) he or she could disrobe in privacy without being concerned that an image of his/her private area was being captured, or b) any part of his/her private area would not be visible to the public, whether such person is in a public or a private place.[31] Where a person lawfully secures access to any electronic record, book, register, correspondence, information, document or other material and discloses such electronic record, book, register, correspondence, information, document or other material to any other person without the authority of the person concerned, he shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or both.[32] But surprisingly there is no provision for imprisonment or fine for simple breach of privacy committed by an individual.

VII. CONCLUSION

India has no independent legislation on Data Protection. The existing legal principles are yet to be tested in cyberspace as the courts have not yet found any direct opportunity to decide any case involving privacy issues of cyberspace. The only inference which one could draw from the existing precedents involving other technologies is that courts are stressing on procedural safeguards and are shying away from establishing substantively limits of the state's power to circumvent right to privacy. The IT Act has laid down procedure for interception, monitoring and decryption of the information and imposed criminal liability on any person who captures image of the private part of any person. Similarly, any person who has got information lawfully but discloses it without the authority of the person concerned will be punished but there is no provision for imprisonment or fine for simple breach of privacy committed by an individual.

[30] Supra note 27
[31] Section 66E
[32] Section 72

REFERENCES

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 Harv.L.Rev. 193 (1890).

[2] William L. Prosser, "Privacy", CAL. L. REV., 48, (1960), pp. 383.

[3] Monteleone, Share, "Ambient Intelligence and the Right To Privacy: The challenges of Detection Technologies," European University Institute, DOI:10.2870/24183.

[4] S. Gutwirth, "Biometrics between Opacity and Transparency," Annuali dell'Istituto Superiore di Sanita, 43(1), (2007), pp. 61-65.

[5] Lipton, J. D., "Mapping Online Privacy," Case Western Reserve University School of Law, Case Research Paper Series in Legal Studies Working Paper (2009), pp. 09-24.

[6] Shrikant Ardhapurkar et al. "Privacy and Data Protection in Cyberspace in Indian Environment," International Journal of Engineering Science and Technology, 2(5), (2010), pp. 942-951.

[7] O'Hara, K. and Shadbolt, N., "The Spy in the Coffee Machine: The End of Privacy As We Know It," One-world, Oxford, (2008).

[8] Jacqueline D.L., "Mapping Online Privacy," 477 N.W. U. L Rev., 140, (2010), pp. 481-82.

[9] Johnson, B., "Privacy no longer a social norm, says Facebook founder," Guardian, 11th Jan, (2010).

[10] Daniel J.S., "A Taxonomy of Privacy," 154 U. PA. L. REV., 477, (2006), pp. 482-483.

[11] Joel R.R., "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? ," 44 Fed. Comm. L.J. (1992), pp. 195.

[12] Zuac L., "Constitutional Dilemmas," Oxford University Press, (2008).

[13] Van Der Schyff, G., "Limitation of Rights," Wolf Legal Publisher, Nijimegen, (2005), pp. 228.

 ISBN: 978-1-61208-182-3