

THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008: THE PROVENANCE OF E-POLICING

Sakshi Sawhney*

Abstract

A long time ago, in the year 1949 to be more precise- a very wise man made a prophecy. This man was George Orwell, who in his book 1984 spoke of the terrors unleashed by an ubiquitous and omniscient Government known as the “Big Brother”. This article examines the materialisation of Orwell’s prophecy in India where the Parliament passed in twenty two minutes the seemingly beneficial Information Technology Amendment Act, 2008 which in fact bestows powers on the Government that uncannily resemble those of Big Brother. While it is accepted that libertarianism cannot be the policy for governance in a time where national security is at stake, still, one cannot justify the adoption of the other extreme and find a solution in the policy of totalitarianism. This article seeks to demonstrate how the provisions of the Act will denude the citizen in front of the ever mighty Government who will constantly watch its citizen, pry through its e-mails and arbitrarily arrest its citizen for not adhering to the morality of the Government. This article warns of the provenance of e-policing and its consequences if the same is not exercised moderately.

I. INTRODUCTION

The Information Technology Act, 2000¹ was passed with the dual objectives of granting legal recognition to commercial transactions being carried out over the internet and to oversee and regulate other electronic transactions and exchanges. Though the Act was initially hailed as an imperious intervention, several cyber law experts² spoke of the inadequacy of its provisions: it was primarily a legislation enabling e-commerce and not for preventing cyber crimes. Even the preamble of the Act does not mention the prevention of cyber crimes as its purpose.³ The

* Student, III Year, B.A., LL.B. (Hons.), NALSAR University of Law, Hyderabad.

1 Hereinafter referred to as “the Act”.

2 Praveen Dalal, *Cyber Law in India Needs Rejuvenation*. Available at: <http://indianattorney.org/claw.html> (last accessed on 23rd September, 2009); Devangshu Datta, *Big Flaws in Cyber Laws*, December 23rd, 2004, Business Standard. Available at: <http://www.business-standard.com/india/opinion/Individual.php?id=21&total=197&pgno=9> (Last accessed on 4th October, 2009).

3 “An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers’ Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.....AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records...”- Preamble, Information Technology Act, 2000.

legislation does not define cyber crimes and hence could not be used for tackling issues such as cyber-stalking and bullying.⁴ Cases such as that of *Avinash Bajaj v. State*,⁵ in which the Act was used to charge the Managing Director of a popular website with personal liability for a third party's advertisement on the website which contained sexually explicit material, sparked off a massive debate regarding the inadequate procedures in the Act and even led to a citizen petition being signed demanding the clarification in the law.⁶ The practical difficulties in applying the Act was also realised by the Supreme Court in *State of Punjab v. Amritsar Beverages Limited*,⁷ which observed that even though several amendments have been made to the Act, it still does not deal with all the problems which are faced by the officers enforcing the said Act such as statutory liabilities, lack of scientific expertise and lack of sufficient insight in dealing with the internet.⁸

All of the aforementioned reasons necessitated a change in the existing cyber law, thus the Information Technology (Amendment) Act, 2008⁹ was passed in order to fill in the gaps left by the prior law. However it is worth asking whether this Act was really the solution to the problems created by the previous legislation, or instead is merely a new problem created by the Legislature.

The Amendment Act was passed by the Parliament on December 23, 2008 in 26 minutes, with hardly any discussion or debate.¹⁰ The consequence was the birth of a legislation which prescribed Big Brother-like functions to be performed by the State. It is remarkable, indeed, that a democratic country like India can possibly witness George Orwell's Nineteen Eighty Four come to life.

While there is no dearth of ambiguous and vague provisions in the impugned Act, the author has focussed on two broad underlying themes, namely surveillance and censorship, which permeate the Act and push the country towards the reality of E-policing.

The impugned provisions of the Amendment Act namely, Section 67, Section 69, Section 69A and Section 69B have been the primary area of focus. The author has tried to bring to light the casuistry that the Legislators have employed to accomplish their ultimate goal of control over the citizens.

4 Shaheen Shariff, *CYBER BULLYING: ISSUES AND SOLUTIONS FOR THE SCHOOL, THE CLASS ROOM AND THE HOME* p. 64 (Routledge Taylor and Francis Group, New Delhi, 1st ed. 2008).

5 150 (2008) DLT 769.

6 <http://www.petitiononline.com/baazee/petition.html> (Last accessed on 23rd September, 2009).

7 AIR 2006 SC 2820.

8 AIR 2006 SC 2820 at para 7.

9 Hereinafter, "Amendment Act".

10 Times of India, Amid Din, LS passes 8 bills in 17 minutes without Debate, 24th Dec. 2008, New Delhi.

The paper has been divided in the following two parts: surveillance and censorship. In the first part, the author has examined the difference between the surveillance provision in the Act of 2000 and the Amendment Act. The law of privacy in India, the United States and the United Kingdom has been examined, and a case has been made for the internalisation of the respect for privacy in law as it affects both the individual and the society in terms of several rights, such as the freedom of speech and expression. The author has discussed the nature of unfettered powers vested on the officials to take away society's right to privacy.

In the second part of the paper, the author has discussed censorship and how it impacts the privacy of society. The subjectivity in the test of what is obscene and the liability placed on intermediaries in this respect has been looked into. The author has also contended that the provisions of obscenity as laid down by the Amendment Act are very different from the law of obscenity that prevails as of today under the Indian Penal Code. The author concludes by contending that the law makers in India need to balance the right of security of the society with that of the right of privacy in order to prevent the democratic pillars of India from collapsing to give way to a police state.

II. SURVEILLANCE

“There can be no justification for this gradual but incessant creep towards every detail about us being recorded and pored over by the state.”¹¹

A careful reading of the statement of objects and reasons of the Act¹² gives the subtle allusion to prevention of cyber terrorism, which is the government's rationale behind amending Section 69 of the Information Technology Act, 2000. However, nothing in the statement of objects and reasons prepares one for the consequences of the amendment. One of the primary reasons for amending the Information Technology Act, 2000 was because its provisions were seen to be iniquitous and intrusive.¹³ In fact, Section 69 of the Act of 2000,¹⁴ which empowered the government

11 Lord Goodlad, *Chairman of House of Lords Select Committee into Privacy, Surveillance and the Effects on Civilians*, reported in BBC News, WARNING OVER ‘SURVEILLANCE STATE’, 6th Feb. 2009, London. http://news.bbc.co.uk/2/low/uk_news/politics/7872425.stm, (last accessed on 23/July/2009).

12 “The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.”- Statement of Objects and Reasons of the Information Technology Amendment Act, 2008. Available at : http://www.mit.gov.in/download/it_amendment_act2008.pdf (last accessed on 23rd September, 2009).

13 Arunabh Ghosh and Nandan Kamath, *Is Internet Really the Leveller?*, India Together (August, 2002). Available at: <http://www.indiatogether.org/opinions/scitech/ddivide.htm> (Last Accessed on 4th October, 2009).

14 “69. Directions of Controller to a subscriber to extend facilities to decrypt information.

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for

to intercept electronic data, has been arraigned for violating the civil liberties of the citizens.¹⁵ However, instead of rectifying the provision, the newly amended Section 69 goes a step further in allowing the government access to any information and correspondences being sent or received via the internet.¹⁶

A comparison of the old and the new provisions will reveal the extent of intrusion that the government has been empowered to undertake under the new provision. The new provision allows the government to intercept and watch over electronic communications in order to investigate any offence regardless of its gravity and has also expanded its ambit to include “any information generated, transmitted, received or stored in any computer resource”. It permits not just decrypting and intercepting of information but also monitoring of the internet. The Amendment Act, 2008 has thus added two new provisions - Section 69 A and Section 69 B in furtherance of this broader objective of surveillance.

Although ostensibly these new provisions and amendments present an ‘only if necessary’ outlook, they are a culmination of already intrusive behaviour of the government. This is because, the sole practical and efficient mechanism for the government to acquire information and monitor any e-correspondences or their authors that are a probable threat (to the sovereignty or integrity of India, defence of the country, security of the state, foreign relations or are capable of the incitement of any cognisable offence),¹⁷ is by means of setting up content filters¹⁸ or ‘packet sniffing programmes’ on the internet.¹⁹ These content filters search for specific terms in the correspondences taking place over the internet, such as ‘kill’, ‘Lashkar-e-taiba’ and the like. Once a correspondence of this nature is intercepted, regardless of its context, the sender or receiver or both will be under surveillance.

preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.”- Section 69 of the Information Technology Act, 2000.

15 Sruti Chaganti, *Information Technology Act: Danger of Violation of Civil Rights*, The Economic and Political Weekly 13 (23rd August, 2003).

16 “69. (1) Where the Central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.”-Section 69 of the Information Technology Amendment Act, 2008.

17 Section 69(1) of the Amendment Act, 2008.

18 Richard A. Posner, *Privacy, Surveillance and Law*, 75 U.Chi.L. Rev.245 (Winter, 2008).

19 Alexander Dias Morgan, *A Broadened View of Privacy as a Check against Government Access to E-mail in the United States and the United Kingdoms*, 40 N.Y.U.J Int'l L. & Pol. 803 (Spring 2008).

Thus, the mechanism that Section 69 of the Amendment Act, 2008 envisages is one of a perennial nature, a permanent measure of e-mails; this is betrayed by the legislation not only in its object of ‘preventing the incitement of a cognizable offence’ but also through its objective of monitoring of electronic information.

The United States has two separate legislations²⁰ that deal with surveillance of electronic correspondences through these ‘packet sniffing programmes’.²¹ The United Kingdom also employs these surveillance programmes through its Regulation of Investigatory Powers Act, 2000.²² However these legislations are also being criticised for their boundless intrusion into the privacy of their citizens.²³

The full import of the cleverly worded section raises eyebrows as one realizes the magnitude of the citizen’s privacy being sacrificed at the altar of national security. It is pertinent at this stage, to delve into the concept of privacy and the dangerously wrong notions of privacy that are held by law makers and the guardians of law.

A. DEFINING PRIVACY

Privacy has been defined in terms of personhood to be “a distinctive conception of private life as a haven from State power.”²⁴ It was famously held in the dissenting opinion of Justice Brandeis in *Olmstead v. United States*²⁵, that the right to privacy is the “right to be let alone” and he privileged it by stating that it is “the most comprehensive of rights and the right most valued by civilised men”. In 1990, the Calcutt Committee in its report entitled, Report of the Committee on Privacy and Related Matters, defined privacy to mean “the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.”²⁶ Privacy can be best described as propounded by Edward S. Corwin as “Liberty against Government.”²⁷

Privacy as a right has not been expressly recognised by the Constitution in India but belongs to the genre of rights that have been read into various Fundamental

20 The Electronic Communications Privacy Act, 1986 (consisting of three subparts: The Wiretap Act, The Stored Communications Act and the Pen Register Act.) and Foreign Intelligence Surveillance Act, 2006.

21 Alexander Dias Morgan, *A Broadened View of Privacy as a Check against Government Access to E-mail in the United States and the United Kingdoms*, 40 N.Y.U.J Int’l L. & Pol. 803 (Spring 2008).

22 <http://security.homeoffice.gov.uk/ripa/about-ripa/> (Last Accessed on 4th October 2009).

23 James Risen and Eric Lichtblau, *E-mail Surveillance Renews Concerns in Congress*, The New York Times, 16th June, 2009, Washington D.C. Available At: <http://www.nytimes.com/2009/06/17/us/17nsa.html> (Last Accessed on 4th October, 2009); Stefano Ambrogi, *Public Spied on 1,500 Times a Day in UK*, Thomson Reuters, 10th August, 2009, London. Available at: <http://www.reuters.com/article/internetNews/idUSTRE5792JC20090810> (Last Accessed on 4th October, 2009).

24 Stephen J. Schnably, *Beyond Griswold: Foucauldian and Republican Approaches to Privacy*, (1991) 23 C L. R. 861. 25 277 US 438 (1928).

26 HC Deb 21 June 1990 vol 174 cc 1125-34.

<http://hansard.millbanksystems.com/commons/1990/jun/21/calcutt-report#1990-06-21T16:10:00Z>.

27 Edwards S. Corwin, LIBERTY AGAINST GOVERNMENT i (1948) .

Rights. The same position holds true even in the United States and the United Kingdom and as terrorism is a global enemy it is only pertinent to examine these laws as well as other international laws in our discussion.

Privacy has been recognised as a necessary human right of the denizens of the world in various international conventions. For instance, Article 12 of the Universal Declaration of Human Rights has stated that all persons shall have protection against attacks on their privacy.²⁸ The right to privacy has also found sanctuary in Article 17 of the International Covenant of Civil and Political Rights which states that no person shall be subject to arbitrary interference with his privacy including his correspondences.²⁹ Further evidence need not be proffered to establish that privacy is an important prerequisite of the human and is a fundamental part of his or her liberty. Liberty, as has been observed in the celebrated judgment of *Munn v. Illinois*,³⁰ is not ‘mere animal existence.’

B. PRIVACY LAWS IN USA AND UK

Privacy law in India, USA and the UK has primarily developed through a series of judicial decisions concerning surveillance by the State. A look at the history of search and surveillance laws proves that these have always involved issues of privacy; for instance, in the landmark decision in *Seymane’s case*³¹ it was laid down that ‘Every man’s house is his castle.’ Again, in the House of Lords decision of *Entick v. Carrington*³² where the agents of the King had broken into the house of John Wilkes to locate controversial pamphlets defaming the King and in the process had broken into his drawers and lockers, the Court held that the behaviour was ‘subversive of all comforts of society’ and was ‘contrary to the genius of the law in England.’ The case held that the right to privacy protected trespass against property.

Thereafter, the 4th Amendment to the Constitution of the United States was passed in 1791 and was reflective of the aforementioned English cases. It states that:

“The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be

28 Article 12, The Universal Declaration of Human Rights, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” <http://www.un.org/en/documents/udhr/>, (last accessed on 23rd July 2009).

29 Article 17, International Covenant on Civil and Political Rights, “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.” <http://www2.ohchr.org/english/law/ccpr.htm>, (last accessed on 23rd July 2009).

30 94 US 113 (1877).

31 (1604) 77 Eng. Rep. 194 (KB) referred in *Distt. Registrar and Collector, Hyderabad v. Canara Bank*, AIR 2005 SC 186.

32 (1765) 95 Eng. Rep. 807.

violated and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

This amendment nowhere mentioned the right to privacy of a person and the USA, like UK, recognised privacy only with regard to property such as in the case of *Boyd v. United States*.³³ After 40 years, the first case of surveillance that was challenged on the grounds of the 4th Amendment was *Olmstead v. United States*³⁴, wherein the majority opinion was that surveillance was not a matter to be dealt with under the 4th Amendment. As mentioned previously, it was Justice Brandeis’ dissenting opinion that became famous in establishing the first link between privacy of person against surveillance and the 4th Amendment. He observed that:

“The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness... They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed must be deemed a violation of the Fourth Amendment.”³⁵

In the case of *Griswold v. State of Connecticut*,³⁶ it was held that the right to privacy emanated out of the right to freedom of speech and expression. It was further held that the various guarantees created ‘zones of privacy’ and that the protection against all Government invasions ‘of the sanctity of man’s house and the privacies of life’ was fundamental. It was the case of *Warden v. Hayden*³⁷ that drew a clear link between the 4th Amendment and the right to personal privacy wherein it was recognised that the 4th amendment dealt with the right to privacy more than that of property. The famous judgment of *Katz v. United States*,³⁸ held that the Fourth Amendment protected ‘people and not places.’ Harian J. concurred and stated that the protection guaranteed by the Fourth Amendment would be triggered whenever

33 (1886) 116 US 616 (627).

34 (1928) 277 US 438. The Court decided on the question of whether wiretapped telephone conversations used as evidence constituted a breach of the defendant’s rights under the Fourth and Fifth Amendments. The majority decision held that this was not the case as “The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.” The decision was subsequently repealed in *Katz v. United States*, 389 US 347 (1967).

35 *Id.* at 478.

36 (1965) 381 US 278.

37 (1967) 387 US 294 (304).

38 (1967) 389 US 347.

investigations invaded a ‘reasonable expectation of privacy.’

C. PRIVACY LAW IN INDIA

In India, the earliest case to establish the connection between privacy and surveillance was that of *Kharak Singh v. State of UP*,³⁹ wherein domiciliary visits at night at the house of an accused were challenged as a violation of the right to privacy. Subba Rao J. while holding the domiciliary visits as invalid, in his concurring opinion also observed that, although the Constitution does not expressly refer to the right to privacy, it can be traced from the right to life under Article 21 as well as the right to freedom of speech and expression under Article 19 (1)(a). The next case of equal importance is that of *Govind v. State of MP*,⁴⁰ wherein a more practical approach was employed and it was held that while the right to privacy did exist, it was not an absolute right and could be restricted only when there was a superior and ‘compelling state interest’. Further, the case of *Malak Singh v. State of Punjab*⁴¹ held that it was “necessary to satisfy the court that there are grounds to entertain such reasonable beliefs that there is no illegal interference in the life of the citizen under the guise of surveillance”. The court also held that:

“Surveillance cannot squeeze the fundamental freedoms guaranteed to all citizens or obstruct the free exercise and enjoyment of those freedoms nor can the surveillance so intrude as to offend the dignity of the individual. Surveillance of persons... for reasons unconnected with the prevention of crime, or excessive surveillance falling beyond the limits prescribed by the rules will entitle a citizen to the Court’s protection which the Court will not hesitate to give.”⁴²

D. INTERNALISING THE RESPECT FOR PRIVACY

The discussion above lays down two important aspects that will buttress the contentions of the author, namely, that the right to privacy has been recognised as an important factor even in cases of surveillance and secondly that this right can be curtailed in case there is an important State interest at stake. In fact in England, post the Calcutt Report on Privacy, the Press Complaints Commission was established and a code of conduct was formulated for the regulation of the press.⁴³ This code states that the press should respect the privacy of digital communications of a person.⁴⁴ But even the media’s respect for privacy is qualified. The exception arises in the

39 AIR 1963 SC 1295.

40 AIR 1975 SC 1378.

41 AIR1981 SC 760.

42 AIR1981 SC 760 at para 9.

43 Sallie Spilsbury, *MEDIA LAW*, (Routledge Cavindish, 2000) 318.

44 “i) Everyone is entitled to respect for his or her private and family life, home, health and correspondence, including digital communications. Editors will be expected to justify intrusions into any individual’s private

interest of public justice, which is inclusive of the detection of any crime or its exposure, in which instance the press can be exempted from observing the respect for privacy condition.⁴⁵ If that be the case, the State would most definitely be entitled to breach one's privacy if it has a legitimate and compelling reason to do the same. It would also be ridiculous to contend that terrorism is not a compelling state interest. However, it is discernable that the right to privacy has not even been internalised in the impugned legislation so that there may be a balance between the two. This was pointed out even by the Parliamentary Standing Committee in its report on the Amendment Act.⁴⁶

The compelling need for the internalisation of the respect for privacy is the fact that privacy, being predominantly an individual's interest, can easily be denied or sacrificed instead of imposing a mere restriction or curtailment. This will put the right to privacy 'on the defensive'.⁴⁷ It has been contended that the right to privacy is not just in the interest of the individual but that of the society as well. For instance Professor Anthony Amsterdam has argued that privacy protection may be viewed as 'a regulation of government conduct' and thus as a 'regulatory canon' that keeps us 'collectively secure'.⁴⁸

Professor Roger Clarke⁴⁹ has stressed that in this world of 'dataveillance', dangerously gargantuan consequences will result in storing large amounts of data at both the individual and the societal levels.⁵⁰ He has identified the consequences to the individual to include "witch hunts, inversion of the onus of proof, ex-ante discrimination and guilt prediction, unknown accusations and unknown accusers"; the consequences to be borne by society include "prevailing climate of suspicion, adversarial relationships, increasing tendency to opt out of the official levels of society and the repressive potential for a totalitarian government."⁵¹

life without consent..." Press Complaint Commission, Code of Practice. <http://www.pcc.org.uk/cop/practice.html> (last accessed on 23rd September, 2009).

45 Press Complaint Commission, CODE OF PRACTICE. <http://www.pcc.org.uk/cop/practice.html> (last accessed on 23rd September, 2009).

46 Standing Committee on Information Technology (2007-2008), FIFTIETH REPORT ON THE INFORMATION TECHNOLOGY AMENDMENT BILL, 2006, Presented to Lok Sabha on 7.9.2007, 26. <http://164.100.47.132/committeereports/Information%20Technology/REPORT-I.T.-50E.pdf> (last accessed on 23rd September, 2009).

47 Alexander Diaz Morgan, *A Broadened View of Privacy as a Check against Government Access to E-mail in the United States and the United Kingdoms*, 40 N.Y.U.J Int'l L. & Pol. 803 (Spring 2008).

48 Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 367 (1974).

49 Visiting Professor - Cyberspace Law and Policy Centre, Faculty of Law, University of N.S.W; E Commerce Programme, Faculty of Engineering, University of Hong Kong; Department of Computer Science, Australian National University; Institut für Wirtschaftsinformatik, Johannes-Kepler-Universität Linz; Institut für Wirtschaftsinformatik, Universität Bern.

50 Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (May 1998).

51 Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (May 1998). Also refer to A. Michael Froomkin, *Death of Privacy?*, 52 Stan. L. Rev. 1461 (2000).

Thus if societal interests in privacy had been kept in mind rather than the dangerous notion of individual privacy, the result would have been a more balanced legislation which provided for safeguards for privacy even in the circumstances of the compelling state interest.

E. PRIVACY VERSUS SURVEILLANCE

Consequently a perilous paradox arises wherein the lack of protection to societal privacy by the legislation goes against the principles of democracy which this anti-terror provision seeks to defend in the first place. Our democratic society prides itself on the freedom of speech and expression guaranteed to the citizens under Article 19(1)(a). However, as explained earlier, the content filters catch on to words such as ‘terrorism’, politician names and such other expressions thereby triggering off surveillance. This results in the establishment of a Benthamian internet Panopticon⁵² whereby the observed (prisoner) does not know when he is being observed and thus tries to conform his behaviour to the prescribed form so that he does not attract the attention of prison guards. The consequences of this will be that out of fear of attracting surveillance, persons will refrain from discussing matters of national importance, over which they have a fundamental right to express their opinion. This will lead to not just the stultification of the growth of the society but also in prior restraint of its fundamental right of free speech and expression.

The Hon’ble Supreme Court in the case of *People’s Union of Civil Liberties (PUCL) v. Union of India*,⁵³ held that the right to freedom of speech and expression means the right to express one’s convictions freely by modes inclusive of writing and that the mode of communication by telephone was the employment of this freedom. By similar disposition the mode of communicating via e-mail can also be said to be the exercise of the right to freedom of speech and expression. The effect of this Act is to be a prior restraint on the freedom of speech and expression of the fearful citizens who would refrain from voicing their opinions in order to escape the government’s ‘All Seeing Eye’.

The case of *R. Rajagopal v. State of Tamil Nadu*,⁵⁴ relied on the judgment given in *New York Times v. United States*⁵⁵ in order to hold that officials do not have the authority to impose prior restraint on the Freedom of Speech and Expression of a person in the apprehension of defamation. In the case of *Madhu Limaye v. Sub-divisional Magistrate*⁵⁶ it was held that a prior restraint of the Freedom of Speech and

⁵² The Panopticon is a model prison developed by Jeremy Bentham wherein a centralised surveillance tower is embanked by prison cells and the prisoners do not know when they are being watched and hence try and regulate their behaviour. See, Michel Foucault, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON, 195 (1995).

⁵³ AIR 1997 SC 568.

⁵⁴ (1994) 6 SCC 632.

⁵⁵ 403 U.S. 713 (1971).

Expression is per se unreasonable and against the Constitution unless it falls under the exception of Section 144 of the CrPC or even cinematography.⁵⁷

The impugned provision is clearly a pre-restraint on the freedom of speech and expression and is also colourable. It has been held in several cases⁵⁸ such as that of *Kesavananda Bharati v. State of Kerala*,⁵⁹ that what the Legislature cannot do directly it cannot do indirectly: the effect of the present Act is nothing but indirect and unreasonable curtailing of the freedom of speech and expression of the citizens.

While it might be questioned as to how one can claim email correspondences to be private because they are made available to third persons namely the server and that if one doesn't want to fall under the surveillance mechanism, one should just not assume the risk. However, with an estimated forty-eight million users in India,⁶⁰ the importance of the internet in the life on an individual cannot be emphasised enough. Further, as Professor Tribe has observed that "one can hardly be said to have assumed a risk of surveillance in a context where as a practical matter, one had no choice."⁶¹

Further, there is no guarantee that the objective of the provision of fighting terrorism will be met by this drastic step of monitoring all email correspondences. The world has witnessed through various terror strikes that it is engaging with an immensely shrewd antagonist. It is clear that email accounts can be made on false names, code words can be developed for correspondences to take place online and one person or organisation may create a plethora of email addresses for its use. It will not be the enemy that will talk openly of national terror strikes but the citizen who wishes to express his opinion.

F. UNREASONABLE LIABILITY AND PROCEDURE

Another problematic aspect is Section 69(4)⁶² which states that a subscriber or intermediary or any person who does not assist and cooperate with the agency empowered to intercept, monitor and decrypt electronic information shall be punished with imprisonment for a term which may extend to seven years and shall

56 AIR 1971 SC 2486.

57 *S.Rangarajan v. P.Jagjivan Ram*, (1989) 2 SCC 574.

58 *Saru Rural and Urban Welfare Society v. Union of India*, 2009 (11) SCALE 278 at para 43; *Ramdev Food Products Pvt. Ltd. v. Arvindbhai Rambhai Patel*, (2006) 8 SCC 726 at para 73; *Shiv Kumar Sharma v. Santosh Kumari*, AIR 2008 SC 171 at para 18.

59 (1973) 4 SCC 225.

60 Paul Budde Communication Pty Ltd., India-Key Statistics and Telecommunications Market Overview, 2 (2006) <http://www.budde.com.au/Research/India-Key-Statistics-and-Telecommunications-Market-Overview.html> (last accessed on 23rd July, 2009).

61 Discussed in *Distt. Registrar and Collector, Hyderabad v. Canara Bank*, AIR 2005 SC 186.

62 "(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."- Section 69(4) of the Information Technology Amendment Act, 2008.

also be liable to fine. This provision has not made any exemption for the press and media and can be employed to coerce the media into revealing their confidential sources of information.⁶³ An even more problematic issue is that the “subscriber” could be an accused himself and compelling him to assist the agency in decrypting information (in CrPC as well the place where the search is conducted the inhabitant is expected to assist the police) available on his computer system would be violative of Article 20(3) of the Constitution as it could lead to the accused bearing witness against himself.⁶⁴

It has been laid down by the Supreme Court in the case of *V.S. Kuttan Pillai v. Ramakrishnan*,⁶⁵ that if the accused is compelled to give information even in the investigation process it would amount to a violation of Article 20(3). In the same case the Court also held that “A passive submission to search cannot be styled as a compulsion on the accused to submit to search... immunity against self-crimination extends to any incriminating evidence which the accused may be compelled to give.”⁶⁶ the process contemplated under Section 69(4) is one requiring ‘assistance’ and ‘cooperation’ of the subscriber, hence it is evidently a participatory process and not a mechanical process which could proceed in the absence of the subscriber.

Further, a comparison with the Code of Criminal Procedure, 1973 shows that the impugned clause is coterminous with Section 39⁶⁷ of the Code as regards providing information as to the commission of any offence, or even sections 91 and 92 of the Code which deal with the production of documents.⁶⁸ However, the maximum punishment for disobedience under Sections 175 and 176 has been fixed at 1 month.⁶⁹ Thus, it is arbitrary and unfair that the penalty for disobedience under the present Act has been fixed at 7 years when the liability is much lesser under the Indian Penal Code and the Criminal Procedure Code.⁷⁰

63 Pranesh Prakash, COMMENTS ON THE DRAFT RULES UNDER THE INFORMATION TECHNOLOGY ACT, The Centre for Internet and Society. <http://www.cis-india.org/advocacy/igov/comments-draft-rules>.(last accessed on 23rd September, 2009).

64 *Ibid.*

65 AIR 1980 SC 85.

66 *V.S. Kuttan Pillai v. Ramakrishnan*, AIR 1980 SC 85 at para 14.

67 “(1) Every person, aware of the Commission of, or of the intention of any other person to commit, any offence punishable under any of the following sections of the Indian Penal Code (45 of 1860), namely..... Shall, in the absences of any reasonable excuse, the burden of proving which excuse shall lie upon the person so aware, forthwith give information to the nearest Magistrate or police officer of such Commission or intention.”

68 Pranesh Prakash, Comments on the Draft Rules under the Information Technology Act, The Centre for Internet and Society. <http://www.cis-india.org/advocacy/igov/comments-draft-rules>.(last accessed on 23rd September, 2009).

69 *Ibid.*

70 *Id.*

The problematic augmentation of power prescribed by the Amendment Act is similar to those of other countries where these expanding powers have been condemned. Consider Article 8 of the European Convention of Human Rights which states that:

- “1. Everyone has the right to respect for ... his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

The decisions of the European Court of Human Rights at Strasbourg in France, though binding only on the parties to the dispute, have determined Human Rights Jurisprudence in various countries such as the U.K.⁷¹ The Court in its interpretation of Article 8 has held that the law should “indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities.”⁷²

The provisions of the Act have conferred upon the executive a demonic power of colossal discretion wherein the omnipresent Government in its cloak of invisibility can glean information about the most intimate, publicly harmless and well guarded secrets of an individual. The Indian Telegraph Act of 1885 which has been said to be one of the most intrusive legislations of the British Raj,⁷³ is one of the primary sources of inspiration for the impugned Act. Section 5 of the Telegraph Act gave narrower but similar powers to the executive as regards phone tapping in the case of a public emergency. However, neither did it define the term ‘public emergency’, nor did it provide any guidelines to the executive.

The Act was thus challenged before the Supreme Court of India in the celebrated case of *People’s Union for Civil Liberties v. Union of India*,⁷⁴ wherein it was held that the executive did not have the authority to exercise its power under Section 5 unless a public emergency occurs or the same is in the interest of public safety. The Supreme Court thereafter defined the terms ‘public emergency’ and ‘public safety’ and went on to lay down guidelines so that citizens could be protected from the arbitrary exercise of State power.

71 Alexander Diaz Morgan, *A Broadened View of Privacy as a Check Against Government Access to E-mail in the United States and the United Kingdom*, 40 N.Y.U.J. Int’l L. & Pol. 803 (Spring 2008).

72 *Rotaru v. Romania*, 8 B.H.R.C. 449, P 61 (Eur. Ct. H.R. 2000).

73 Indian Express, *Yes, Snooping’s Allowed*, 6th February, 2009.

74 AIR 1997 SC 1203.

However, not only has the Amendment Act cleverly decided against adopting the terms ‘public emergency’ and ‘public safety’, it has also forborne from adopting the guidelines laid down by the Supreme Court of India. The Legislature has in fact chosen to widen the ambit of intrusion by permitting the Government to include the investigation of any offence under Section 69.

Such unfettered and arbitrary power can lead to drastic consequences, whereby, the Government can obtain knowledge of the religious and political choices and affiliations of an individual. In the case of *Sudhir Chandra v. Tata Iron and Steel Co. Ltd.*,⁷⁵ the Supreme Court observed that the Constitution of India “envisaged a society governed by the rule of law. Absolute discretion uncontrolled by guidelines which may permit denial of equality before law is the antithesis of rule of law” and thus violative of Article 14. It was held in the case of *State of West Bengal v. Anwar Ali Sarkar*,⁷⁶ that when discrimination is inbuilt in the Act itself, the statute can be struck down as unconstitutional.⁷⁷

Once the Legislation has undermined and taken away these rights of privacy, even if done primarily keeping in mind the objective of achieving national security, the consequence is grave because such an omission empowers the State to permeate other aspects of ones life as well. The impugned legislation is the best example of such a situation because its casual and irresponsible treatment of privacy protection has permitted the State to control aspects of an individual’s life including his choices and lifestyle, which are most private to the individual. The Act has legitimised the State’s action of imposing its notions of morality and decency upon the populace through censorship.

III. CENSORSHIP

“Promiscuous reading is necessary to the constituting of human nature. The attempt to keep out evil doctrine is like the exploit of that gallant man who thought to keep out the crows by shutting his park gate....Give me the liberty to know, to utter and to argue freely according to conscience, above all liberties.”⁷⁸

The terms ‘decency’ and ‘morality’ are vague and elastic notions which vary from country to country depending on the standards of morals of contemporary society,⁷⁹ which vary even within the same country, particularly one as socially disparate and culturally diverse as India, where there are widely varying standards

75 AIR 1984 SC 1064, 1071.

76 AIR 1952 SC 78.

77 Justice Chandrashekhar Iyer’s opinion at para 75(d).

78 John Milton, *AEREOPAGATICA*, (1644).

79 *Chandrakant Kalyandas Kakodkar v State of Maharashtra*, (1969) 2 SCC 687.

of moral acceptability. Courts have gone a step ahead and distinguished between obscenity and pornography and it has been held that pornography denotes writing, pictures intended to arouse sexual desire.⁸⁰

A. SUBJECTIVE SATISFACTION

The general undefined terms ‘indecent’ cover large amounts of non-pornographic material as well. Moreover the standards applied to the internet means that any communication available to a nation-wide audience will be judged by the standards of the community most likely to be offended by the message.⁸¹ Similarly under Section 67⁸² terms like ‘lascivious’ and ‘prurient interest’ do not find any definition in the Act itself and the interpretation of these terms is determined by the subjective views of the officials enforcing the provisions.

According to Easton, both English and American jurisprudence on free speech and censorship are rooted in the democracy and truth justifications of Mill. Underpinning this debate has been the ‘harm principle’ which states that “the only ground on which intervention is justified is to prevent harm to others; the individual’s own good is not a sufficient justification.”⁸³ Neither the expression of pornographic opinions, nor the indulging of a private taste for pornography, causes significant harm to others, in the relevant sense of ‘harm’ (i.e., crimes of physical violence or other significant wrongful rights-violations). Hence, the publication and voluntary private consumption of pornography is none of the state’s business.⁸⁴

Society must lean in favour of speech and expression. There is a definite need to be cautious while upholding restrictions imposed on notions of indecency. The internet age and the breakdown of traditional barriers is rendering censorship easily futile.⁸⁵

80 *Ranjit D. Udeshi v State of Maharashtra*, AIR 1965 SC 881.

81 Epps Garrett, FREE SPEECH ON THE INTERNET, THE FIRST AMENDMENT: FREEDOM OF THE PRESS 238 (2008).

82 “67.Punishment for publishing or transmitting obscene material in electronic form: Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.”-Section 67 of the Information Technology Amendment Act, 2008.

83 http://www.slais.ubc.ca/COURSES/libr500/fall1999/WWW_presentations/C_Hogg/argue.htm (last accessed on 23rd September, 2009).

84 <http://plato.stanford.edu/entries/pornography-censorship/> (last accessed on 23rd September,2009).

85 M.G Divan, FACETS OF MEDIA LAW 64 (Eastern Book Company, Lucknow, 1st ed. 2006).

Further in *K.A Abbas v Union of India*⁸⁶ the Supreme Court of India held that:

“the standards we set for our censors must make a substantial allowance in favour of freedom thus leaving a vast area of creative art to interpret life and society with some of its foibles along with what is good. If the depraved person begins to see in these things more than what an average person would, in much the same way, as it is wrongly said, a Frenchman sees a woman’s legs in everything, it cannot be helped.”

Hidayatullah CJ. criticised the failure of the Parliament and the Central Government to separate the artistic and socially valuable from the obscene and indecent and to appreciate that the artistic and social presentation of an episode could negate its potential to deprave.⁸⁷ The Supreme Court expressed its dissatisfaction that the law was more concerned for the depraved than the ordinary moral man.⁸⁸ In the provisions relating to censorship under Sections 67 and 67A⁸⁹ of the Amendment Act, the question arises, whether the officials are befitted to interpret which material is lascivious or likely to corrupt or deprave? It is the personal morality of the official that will decide whether the picture/content the individual was looking at was lascivious or appeals to prurient interest.

B. ACCESS OF CHILDREN

The Supreme Court has taken notice of the fact that it is children who generally fall under the category of persons likely to be depraved or corrupted by sexually explicit material.⁹⁰ It has been held in the case of *Director General, Directorate General of Doordarshan v. Anand Patwardhan*⁹¹ that it is one of the most controversial issues to balance the protection of society against harm that may flow from obscene material and the need to ensure respect for freedom of expression and to preserve

86 (1970) 2 SCC 780.

87 *Ibid.*

88 (1970) 2 SCC 780.

89 “67A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees. Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form—
(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or
(ii) which is kept or used bona fide for religious purposes.”

90 *Ajay Goswami v. Union of India*, AIR 2007 SC 493.

91 AIR 2006 SC 3346.

a free flow of ideas. However, it was observed by legal realist, Jerome Frank, that Law is a reflection of society.⁹² If that be the case, then the Supreme Court's decision in *Ajay Goswami v. Union of India*⁹³ is reflective of the present standards of obscenity in Indian society. The Court, therein held that an imposition of a blanket ban on the publication of certain materials which were sex oriented will lead to a situation where only the needs of children will be catered to and the adults will be deprived of their share of entertainment "which can be permissible under the normal norms of decency in any society."⁹⁴

A similar disposition can be found even in the United States. In 1996 the Congress in the United States passed the CDA (Communications Decency Act) 1996 which made it a crime to transmit or display material 'harmful to minors' on the Internet without affirmative measures to ensure that no minors could see it. Congress again attempted to limit sexual internet speech with Child Online Protection Act (COPA), 1998. The COPA limited its reach to an offense that seemed to draw approval by O'Conner's concurrence: knowingly making sexually explicit communication and purposefully aiming it at minors.⁹⁵ In 2004 the Supreme Court affirmed a temporary injunction against the COPA on the narrow ground that the government had not shown that there were no less restrictive measures (such as software filters) of protecting minors from exposure to sexual material on the internet.⁹⁶ Another argument in addition to protecting children's interest was the 'equally significant' interest in fostering the growth of the internet. The government apparently assumes that the unregulated availability of 'indecent' and offensive material on the internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.⁹⁷ However, this argument in favour of legislating on this issue was dismissed.

Further, Sections 67⁹⁸, 67A⁹⁹, 67C¹⁰⁰ apply to "electronic devices" which includes Short Messaging Service (SMS) and Multi-media Messaging Services (MMS),

92 Marx, 25 (Rodopi, Netherlands, 1st ed. 1997).

93 AIR 2007 SC 493.

94 *Ajay Goswami v. Union of India*, AIR 2007 SC 493 at para 45.

95 *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) wherein the constitutional validity of the CDA (Communications Decency Act) 1996 and CDA (Communications Decency Act) 1996 was called into question.

96 *Ashcroft v. ACLU*, 542 U.S. 656 (2004).

97 M.G Divan, FACETS OF MEDIA LAW 64 (Eastern Book Company, Lucknow, 1st ed. 2006).

98 *Supra* n.16.

99 *Supra* n. 89.

100 "67 C. Preservation and Retention of information by intermediaries:

- (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
- (2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine."

therefore the Government has been empowered to check even explicit messages exchanged between persons, which may accidentally fall into the hands of children and others with an impressionable mind. The Government has such extensive powers under the Amendment Act that it may even be able to maintain a record of such intimate messages as and when it intercepts them.

C. THE IMPACT OF SURVEILLANCE ON PRIVACY AND INTERMEDIARIES

The tradition legal remedies fail to protect what may be called privacy rights of citizens.¹⁰¹ The infamous *Baazee* case¹⁰² provided an opportunity to the State to amend and rectify the loopholes in the IT Act, 2000. Thus, the Amendment Act, 2008 in adding Section 67 B made necessary and positive changes to the law on child pornography. The same, however, cannot be said of the amendments carried out in relation to intermediaries. These amendments have only empowered the Government to further its intrusive agenda while using the ‘intermediaries’ to carry out the same. The IT amendment Act through Section 67C¹⁰³ allows intermediaries to retain information in a manner and for a time-frame to be determined by Central Government which is a direct violation of the right to privacy.

Here again reference can be made to the case of *People’s Union for Civil Liberties v Union of India*¹⁰⁴ where it was held that the right to privacy included the right to hold a telephone conversation in the privacy of one’s own home and that telephone, a form of “technological eavesdropping” infringed the right to privacy. A parallel can be drawn with Section 67C¹⁰⁵ which allows third parties in the form of “intermediaries” store and retain information which individuals are surfing on the net in the privacy of their homes and offices, as violative of the right to privacy. Even the IT Act 2000 did not provide any protection or adequate safeguards against obtaining illegal and unauthorized access to such information.

The Act also directs intermediaries to play an instrumental role in enforcing the moralities of the State against their clientele. A combined reading of Sections 67¹⁰⁶, 67A¹⁰⁷, 67C¹⁰⁸ and Section 79¹⁰⁹ as applicable to intermediaries, in providing

101 VR Krishna Iyer, *ESSAYS ON PRESS FREEDOM*, (Capital Foundation Society, 1996), 97.

102 *Avinash Bajaj v. State*, 150 (2008) DLT 769 - The appellant was the Managing Director of Baazee.com, a website which allows users to sell goods and service. An advertisement for the sale of a video of the sexual encounter of two school children was put up on the website by a user, and the appellant was arrested by the Police in that regard. With regard to intermediary role, the Court held that the appellant was not personally liable for the same and the Company should have been charged under the IT Act, 2000.

103 *Supra* n.100.

104 (1997) 1 SCC 301.

105 *Supra* n. 100.

106 *Supra* n. 16.

107 *Supra* n. 89.

108 *Supra* n. 100.

109 “79. Exemption from liability of intermediary in certain cases:

for punishment for those who publish what is the ambiguous and mysterious ‘lascivious, prurient or depraving and corrupting’ material, have placed the onus on a website and its ‘due diligence’ to judge whether a joke with sexual connotations falls under the ambit of the Act or not. Differentiating between the subtle thresholds laid down by the Act requires judicial application of mind which these websites cannot possibly have. Therefore, in order to ensure that they are exempt from liability as laid down by the conditions in Section 79,¹¹⁰ the websites will remove any content that may have sexual connotations but may not be of the nature specified in Section 67,¹¹¹ thereby, clearly impacting the fundamental right of free speech and expression under Article 19(1)(a).

The matter does not end here. With the passing of this Act it may be seen that obscenity laws in India, namely those provided under Section 292¹¹² of the Indian Penal Code, 1860 so far punished the person selling or distributing or circulating pornographic content. However, Section 66E¹¹³ of the Act in using the term ‘transmit’

-
- (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.
 - (2) The provisions of sub-section (1) shall apply if
 - (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
 - (b) the intermediary does not
 - (i) initiate the transmission,
 - (ii) select the receiver of the transmission, and
 - (iii) select or modify the information contained in the transmission
 - (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf
 - (3) The provisions of sub-section (1) shall not apply if
 - (a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act.
 - (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.”

110 *Ibid.*

111 *Supra* n.16.

112 “Whoever-

- (a) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, reduces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or”-Section 292 of the Indian Penal Code.

113 “66E. Punishment for violation of privacy:

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.”

seems to punish not just the person from whose server the data is sent but also the recipient who initiates the transmission.¹¹⁴ There is no difference between the test of obscenity as laid down in Section 292 of the IPC and that which has been laid down in Section 66 E of the Amendment Act. Hence, it is submitted that it is against the prevailing law of obscenity as well as unreasonable to place the distributor and the viewer of such material on the same pedestal.

Further, the Act punishes any person who browses or downloads pornographic content from the internet regardless of whether it was unintentional or without knowledge of the same. The legislators have clearly not considered those circumstances when one accidentally stumbles over pornographic content, it may be because of pornographic advertisements on music download websites or web searches for terms that are synonyms for pornographic material without intending to search for the same. The penalty for such accidents is harsh, with a fine that could go upto Rs. 10 lakh or even a five year imprisonment.¹¹⁵

The arbitrary and unfettered powers given to the Executive extend to the aforementioned censorship provisions also. A person can be arrested without warrant even if the information stored on the computer was due to accidental pornographic surfing.¹¹⁶

IV. CONCLUSION

“There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct - in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”¹¹⁷

114 *Supra* n. 63.

115 *Supra* n. 16.

116 Amendment to Section 78 of Information Technology Act, 2000: “ 78. Power to investigate offences (Amended Vide ITAA 2008)

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.” Read with Section 80 of the Information technology Act, 2008: “80. Power of Police Officer and Other Officers to Enter, Search, etc:

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.”

117 George Orwell, NINETEEN EIGHTY FOUR, 9 (1995).

The Amendment Act, makes one apprehensive of the degree of control the Government will wield over our lives in the future, especially when we will be denuded without our garment of privacy. The Act is in fact the provenance of e-policing, thereby, enabling the State to oversee all of ones activities and permeate into ones life. In this regard, the author dealt with two problematic aspects of the draconian legislation, namely, surveillance and censorship. As regards surveillance, in order to balance out the needs of security and privacy, it would be advisable to include within the Act a provision for ex-ante judicial review. One can learn from the mistakes of the knee-jerk, anti-terror surveillance mechanisms established by the US in the form of special tribunals and ex-post judicial review.¹¹⁸ Although the Act does provide for a Cyber Appellate Tribunal, however, under Section 69¹¹⁹ as long as the order for surveillance is given in writing it need not be subject to review. Further, there are many advantages of ex-ante judicial review as opposed to ex-post judicial review, these include the opportunity to curb possible abuse of power; further, judgments will not be obfuscated by the evidence already collected by the surveillance.¹²⁰

Another solution that the author proposes in order to harmonise the apparent conflict between privacy and national security is to build mechanisms within the Act to safeguard privacy. While in many other countries like United Kingdom where there are a new variety of statutes in place that seek to protect these rights like the Privacy Act, 1988 and the Data Protection Act 1988, Indian laws on the subject lag far behind.¹²¹

As evidenced by the censorship provisions, law makers in India have dealt with privacy in a very insensitive manner. While the Act should retain its provisions on child pornography, other arbitrary provisions must be clarified or amended. The State has wrongly taken the Act as an opportunity to enforce its morals on the denizens of the internet-age. It has been observed in the case of *Stanley v. Georgia*,¹²² the state cannot tell a man sitting in the privacy of his house as to what books he may read or what films he may watch. Similarly, the State cannot with its unfettered power enforce upon its citizens a morality in which it believes. No harm is caused by an individual watching what he likes in the privacy of his house and thus the provisions of the Act must be reconsidered in this light.

118 Diaz Morgan, *A Broadened View of Privacy as a Check against Government Access to E-mail in the United States and the United Kingdoms*, 40 N.Y.U.J Int'l L. & Pol. 803 (Spring 2008).

119 *Supra* n.16.

120 *Supra* n. 118.

121 M.G Divan, FACETS OF MEDIA LAW 127 (Eastern Book Company, Lucknow, 1st ed. 2006).

122 (1969) 394 US 557.

If the draconian Legislation had provided a system of checks and balances while allowing for and respecting the need of every individual to keep to himself, it would have been one of a benevolent nature and of democratic character.

It is surprising that even though India is a member of a plethora of international human rights conventions that see every human as an end in himself and guarantees him his privacy, it has still not fulfilled its obligations under Article 51(c) of the Constitution which expects of the State to ‘foster respect for international law and treaty obligations’.

The Amendment Act, 2008 has not yet been notified and is fortunately not in force. The author suggests that before the impugned Act causes a catastrophe to the citizens of the country, certain amendments be made to the Act. It is of primordial importance to prescribe guidelines for the exercise of the amplified discretion conferred by the Act. The legislators also need to accommodate the guidelines that have been laid down by the Supreme Court in similar cases such as the *People’s Union for Civil Liberties v. Union of India*¹²³ which dealt with the exercise of similar powers by the State. Importantly, provisions for ex-ante judicial review and, whenever circumstances permit, *ex-ante* hearing of the aggrieved party must be provided for.¹²⁴ The failure to provide for any of the aforementioned mechanisms will lead to a disintegration of the foundations of democracy.

The Government must respect the private lives of its citizens and device methods to straddle the compelling state interest and societal privacy. Otherwise, citizens will find themselves constantly observed in their actions; there will be stunted growth and development of the generations who find themselves in a dystopian state created by legislations such as this. Life will reduce to mere existence with a distant chimera of freedom.

123 (1997) 1 SCC 301.

124 *Maneka Gandhi v. Union of India*, AIR 1978 SC 597; *Swadeshi Cotton Mills v. Union of India*, AIR 1981 SC 818; *K.I. Shepherd v. Union of India*, (1987) 4 SCC 431.