



## Law relating to Electronic voyeurism in India: Eyes behind the mirror

Atin Kumar Das

Assistant Professor in Law, Haldia Law College, West Bengal, India.

### Abstract

Since the beginning of civilization, man has always been motivated by the need to improve/ enhance the existing technologies. This has led to tremendous development and progress. Of all the significant advances made by mankind till date, probably the most important is the development of Internet. The real power of today's Internet is that it is available to anyone with a computer and a telephone line. Internet places in an individual's hands the immense and invaluable power of information and communication. Internet usage has significantly increased over the past few years. Internet is believed to be fully of anarchy and a system of law and regulation therein seems contradictory. However, technology is governed by a system of law and regulation called cyber law.

**Keywords:** information technology, voyeurism, cyber, privacy, India, law

### 1. Introduction

#### 1.1 Meaning of Voyeurism

A 'voyeur' is generally defined as "a person who derives sexual gratification from the covert observation of others as they undress or engage in sexual activities"<sup>[1]</sup>.

A 'Voyeur' is generally defined as "a person, who observes something without participating; one who gain pleasure by secretly observing another's sexual acts"<sup>[2]</sup>.

#### 2. Meaning of Voyeurism under the Criminal Law Amendment Act, 2013

Voyeurism has surfaced in recent times with the advent of internet and social media sites. For the first time, the 153 year-old Indian Penal Code (IPC) now recognizes stalking, sexual harassment and voyeurism (watching a woman engaging in a private act, where she would have expected not be observed) as crimes. Section 354C of the Criminal Law Amendment Act, 2013 states that Sexual Voyeurism is one of the type of Sexual Harassment that has been identified under the Act. The section clearly states that who have been watched, or recorded, without their consent and under circumstances where the victim could reasonably expect privacy, and where the victim's genitals, buttocks or breast have been exposed<sup>[3]</sup>.

#### 3. Analysis of Electronic Voyeurism under the Criminal Law Amendment Act, 2013

Voyeurism is the act of a person who, usually for sexual gratification, observes, captures or distributes the images of another person without their consent or knowledge<sup>[4]</sup>. With the development in video and image capturing technologies, observation of individuals engaged in private acts in both public and private places, through surreptitious means, has become both easier and more common. Cameras or viewing holes may be placed in changing rooms or public toilets, which are public spaces where individuals generally expect a reasonable degree of privacy, and where their body may be exposed. Voyeurism is an act which blatantly defies reasonable expectations of privacy that individuals have about their bodies, such as controlling its exposure to others. Voyeurism is

an offence to both the privacy as well as the dignity of a person, by infringing upon the right of individuals to control the exposure of their bodies without their consent or knowledge, either through unwarranted observation of the individual, or through distribution of images or videos against the wishes or without the knowledge of the victim<sup>[5]</sup>.

#### 3.1 Electronic Voyeurism under Information Technology Act, 2008

The section is deeply influenced and based on Section 1801 of "Video Voyeurism Prevention Act of 2004" a Federal Law of USA dealing with the felonious act of video voyeurism. The section has been introduced in the Information Technology Act, 2000 by IT Amendment Act, 2008 in view of the dramatic advances in the field of video technology aiding covert clicking of photos without the subject even have a hint about it. The insertion of the said section is a specific attempt to prohibit voyeuristic conduct and by corollary, to protect individual privacy. Video Voyeurism is one of the most portentous of the crime that confront us today. Security in the cyber world is one of the most sensitive issues in the gamut of cyber laws. As the internet rapidly enters the home of the common man, through computers, television, cell phones, and so on, it emerges that violation of privacy is not a threat to dot coms and experts, but also the internet community at large. While in many other countries, there are now a variety of statutes to deal with voyeuristic conduct in place that seeks to protect these inviolable rights, India is not lagging behind to check this new form of felony due to the advancement in the technology, the legislature introduced Section 66E vide the Information Technology Amendment Act, 2008 which came into force on 27 October, 2009<sup>[6]</sup>.

#### 4. Critical Analysis of Electronic Voyeurism

The Section recognizes the right of privacy as inviolable and makes the felony punishable with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. The section recognizes the natural human desire of privacy. It deserves respect and particularly in our

society and cultural ethos & values as we know, it deserves legal protection too. The Section 66E IT Act, 2008 recognizes the right to protect the human body from unreasonable and obscene intrusion by surreptitious video technology and adequately protects the individual privacy from the crime of video voyeurism which destroys personal privacy and dignity by secretly videotaping or photographing unsuspecting individuals.

**5. Enforcement Measures of Electronic Voyeurism under IT Laws in India.**

The researcher already discussed some of the laws in India which are tries to protect the voyeurism includes sexual and video or electronic voyeurism under the Information Technology Amendment Act, 2008 but there are other Rules. And Acts were there to deal with the privacy issues on Internet

In this part the researcher seeks to analyze the rules and Acts which are tries to protect Privacy Issues relating to transmission, capture and Distribute.

**6. The Information Technology Act, 2008**

The IT (Amendment) Act, 2008 has been epoch making legislation. The eonic approach has laid down a new legal erection for the enforcement department. It will not be wrong to say that this amendment has been cybercrime friendly and paves the way for an effective, result bearing and comparatively simpler way of investigating cybercrimes. It also depicts the seriousness of law makers regarding cyber security in the country and has taken in its stride most of the difficulties and hardships faced by the law enforcers. The government approach has been two pronged <sup>[7]</sup>.

**Table 1:** Enforcement Measures under Information Technology Laws

Legal Provision under Information Technology (Amendment) Act, 2008	Punishment	Analysis
<p>Under section 66E “Whoever intentionally or Knowingly captures, Publishes or transmits the image of a private area of any person without his or her consent, under the circumstances violating the privacy of that person, shall be punished with imprisonment which may extent to three years or with fine not exceeding two lakh rupees, or with both</p>	<p>Imprisonment which may extent to three years or with fine not exceeding two lakh rupees, or with both. Non- Cognizable &amp; Bailable offences (Punishment upto three Years).</p>	<p>The insertion of the said section is a specific attempt to prohibit voyeuristic conduct and by corollary, to protect individual privacy. Video Voyeurism is one of the most portentous of the crime that confront us today. Security in the cyber world is one of the most sensitive issues in the gamut of cyber laws. As the internet rapidly enters the home of the common man, through computers, television, cell phones, and so on, it emerges that violation of privacy is not a threat to dot coms and experts, but also the internet community at large. While in many other countries, there are now a variety of statutes to deal with voyeuristic conduct in place that seeks to protect these inviolable rights, India is not legging behind to check this new form of felony due to the advancement in the technology, the legislature introduced Section 66E vide the Information Technology Amendment Act, 2008 which came into force on 27 October, 2009</p>
<p>Section 67 of IT Act, 2008 provides “Whoever publishes or transmits or cause to be published or transmitted 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 published on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the extent of second or subsequent conviction with imprisonment of either description for a term which may extent to five years and also with fine which may extend to ten lakh rupees.”</p>	<p>first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the extent of second or subsequent conviction with imprisonment of either description for a term which may extent to five years and also with fine which may extend to ten lakh rupees.” Non – Cognizable &amp; Bailable offences (Punishment upto three Years)</p>	<p>Section 67 of the IT Act permitted only those instances of obscenity which are published, transmitted and caused to be punished or transmitted in the electronic form. It is also mentioned for the CCTV Camera owners (intermediaries) if a camera captures obscene electronic information, the oener of a CCTV Camera can be booked under section 67, but if the camera captures sexually explicit information, it is classified as a non – bailable offence under section 67A, entailing five years of imprisonment and a fine of Rs 10 lakhs.</p>
<p>Section 67A of IT Act, 2008 provides “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</p>	<p>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. Cognizable &amp; Non-Bailable</p>	<p>Punishment for publishing or Transmitting of material containing Sexual Explicit act, etc., in Electronic Form: The net result of Section 67A is that computers and mobile users in India will have to become extremely careful whenever they are either taking photographs or MMSs or videos from their or others mobile phones of sexually explicit acts or conduct.</p>

which may extend to ten lakh rupees.”	offences (Punishment more than three Years).	
Section 79 provides network service providers not to liable in certain cases.	S.79 only refer to statutory liability and does not operate as an all-encompassing exemption from all types of civil or criminal liability.	Under the earlier section, due diligence was required to be used to prevent commission of an offence. Under the amended section, due diligence is required to be used while discharging duties under the act. Moreover, it is curious that parliament felt it necessary to impose both requirement to observe due diligence in discharging statutory duties in addition to empowering the central government to issue guidelines.

**Table 2:** The Government Approach

Regarding Cyber Security	Regarding Investigations of Cybercrimes
Critical Information Infrastructure (CII), Section 70(I) defines the term “Critical Information Infrastructure” means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.	Section 78 has been amended to replace the word “Deputy Superintendent of police” by the word “Inspector”. Section 80 provides inspector to enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed any offence under this Act.
Protected System, Section 70(I) (Amended) defines the term “Protected System” has been enlarged to bring within its ambit the CII.	Section 2(ha) “communication device” means cell phone, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.
National Nodal Agency, Section 70-A, to ensure cyber security in the country there is provision for the establishment of National Nodal Agency.	Section 79-A – this newly added section shall also be of a great help to the enforcement department as it is for the first time that a technological expert has been included to aid the legal procedure [8].
Indian Computer Emergency Response Team (ICERT) According to section 2(iia) of the IT Act, 2000 “Indian Computer Emergency Response Team” means an agency established under sub-section (I) of Section 70-B <sup>[9]</sup> .	Section 84-B for the first time makes abetment of offences under the IT Act an offence. According to Section 84-B if anyone is found guilty of abetting an offence under the IT Act no separate punishment is given for it then he will be punished with the punishment prescribed for the commission of that offence [10].
Monitoring, interception and decryption of data- Section 69 [11], 69-A [12] and 69-B [13], empowers the government to authorise any agency to take these steps as per the rules prescribed by the government. The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 [14].	Attempt is an offence (S. 84-C) inclusion of this offence under the IT Act would be useful as while trying at the computer, like vandalising the data, hacking, in this condition, the accused can be punished for attempt to commit the crime in question [15].

**7. Conclusion**

Privacy, crime and safety of women are intricately linked in any legal system. An essential part of the security of citizens is the safety of their privacy and personal information. If any legal system does not protect the privacy both of body and information of its people, there will always be insecurity in such a system. With the recent debates on women’s safety, several crucial privacy and security issues have been raised, such as the criminalization of voyeurism and stalking, which is a huge boost for privacy rights of citizen in India, and it is hopeful that the government will continue the trend of considering privacy issues along when addressing security concerns for the state.

By and large instances are occurring in India because of the inherent defect the existing law of India. One of the biggest tragedies as far as the legislations in independent India is concerned, is that India does not have dedicated law to protect privacy. Possibly a need for a same never across earlier. However, the judge- made law in India has made some advances in this regard.

It is important to note that the terms “privacy” and “Video Voyeurism” has still not been defined under the amended Information Technology Act, 2008.

Thus it can be concluded that the sending of an MMS capturing the private area of any person thereby violating of his privacy under the parameters detailed under Section 66E of the IT Amended Act, 2008, would also be now brought within the ambit of penalty and punished with imprisonment for a term three years or with fine which may extent to two lakh rupees or with both.

**8. References**

1. Singh Dalla Harpreet. Cyber Crime – A threat to person, property, Government and Societies. IJARCSSE. 2013; 3(5).
2. Prof. Walker MB. Chamber’s Dictionary of Science and Technology, Ed. 4, Allied Chambers, New Delhi India. 2001, 1246.
3. The Criminal Law Amendment Act, DL (N) 2003-13, Ministry of Law & Justice Legislative Department, 2013.
4. Garner Bryan A. Black’s Law Dictionary Ed.1, West Group, USA. 1999, 1572.
5. Available at <http://www.mightylaws.in> (Last visited on 08.09.2016)
6. Section recognizes the right of privacy as inviolable and makes the felony punishable with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. The section recognizes the natural human desire of privacy. It deserves respect and particularly in our society and cultural ethos & values as we know, it deserves legal protection too. The Section 66E IT Act, recognizes the right to protect the human body from unreasonable and obscene intrusion by surreptitious video technology and adequately protects the individual privacy from the crime of video voyeurism which destroys personal privacy and dignity by secretly videotaping or photographing unsuspecting individuals, 2008.
7. Fatima Talat. Cybercrimes, Ed.1, Eastern Book Co. Lucknow. 2011, 438.
8. Inserted by virtue of S. 40 of the IT (Amendment) Act, (10 of 2009) and a new chapter XII-A has been added which

includes the section 79-A *Central Government to notify Examiner of Electronic Evidence*, 2008.

9. Inserted by S.36 of the IT (Amendment) Act, (10 of 2009). The central government shall make arrangements for the establishment of a central entity to serve as ICERT. This will be a specialized body primarily to take care of the protected system in the country, 2008.
10. Inserted by S. 45 of the IT (Amendment) Act,.Abetment is defined under S. 107 of IPC, 1860 as an offence, 2008.
11. Section 69 of IT Act, 2008 provides direction for interception or monitoring or decryption
12. Section 69-A of IT Act. Provides blocking for public access, 2008.
13. Section 69-B of IT Act. Provides monitoring and collecting traffic data, 2008.
14. Vide G.S.R. 782 (E), 2009.
15. Inserted by S. 45 of the IT (Amendment) Act. Attempt is defined under S. 511 of IPC as a punishable offence, 2008.