
PRIVACY ISSUES IN CYBERSPACE: AN INDIAN PERSPECTIVE

***Dr. Gagandeep Kaur**

Assistant Professor in Law (Senior Scale), School of Law, University of Petroleum and Energy Studies, Dehradun, Uttarakhand

---

ABSTRACT

Cyber privacy is controversial and as yet unresolved question in legal jurisprudence all around the world. In the new millennium, the present universe is encompassed by the power of new mantra namely 'Information Technology'. The sempiternity of knowledge in the lap of 'Information and Communication Technology Revolution' has staggeringly brought the privacy of individuals into the forefront of the Jurisprudential consciousness. To what degree citizens of democratic nations would be willing to surrender their sensitive information is debatable. However, it is the responsibility of legal domain to prepare an adequate policy for the protection of privacy on the internet form cyber snooping, cyberstalking, corporate espionage, devasting cyber-attacks and website defacement. The computerization of society has important and possibly unsettling implications that invite a re-examination of the privacy in cyber world. This article has focused on the (i) Analysis of the novice modes of the tarnishing privacy in cyberspace in India and (ii) Legal control mechanism to combat commission of crimes.

Key Words: Cyber Privacy, Cybercrimes, Fundamental Right to Privacy, The Information Technology Act, 2000 (2008).

1. INTRODUCTION

The Information and Communication Technology acts as an inexpensive and abundant fuel, for 'Digital Society' which is global in nature, deeply innovative and dependent on the "Internet Revolution".[1] The explosive growth of hi-tech Computer Science technology and its capacity to gather, store and process copious amounts of personal information has posed grave security threats to vital national infrastructure.[2] This sensitive and seemingly intractable problem of virtually unrestricted internet freedom has complelled to rethink the privacy parameters in the

[1] Graciela Chichilnisky, *The Knowledge Revolution*, 7 J. INT. TRADE ECON. DEV. 39–54 (1998).
[2]Tamara Dinev and Paul Hart, *Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact*, 10 International Journal of Electronic Commerce, 7-29 (Winter, 2005/2006).

cyberworld. [3] As more and more internet users surf the internet and post their personal information; in the form of educational qualification, marital status, private selfies, videos, family photos, hobbies and interests, online on social media networking websites are easily accessible to the general public. This led to the scam of loss of personal data such as the *KOOBFACE*. *KOOBFACE* is a malicious malware and composed of various components, each with specific functionalities. While most malware cram their functionalities into one file, *KOOBFACE* divides each capability into different files that work together to form the *KOOBFACE* botnet.[4] The virtual world has left almost no information private.

Protecting privacy entwines shield to users' personal information to ensure that they have the confidence and ability to take advantageous of the Internet's benefits. Privacy breaches cause a multifariousness of harms, including the exposure of sensible, personal information to unintended sources, and fiscal losses. [5] Each and every mouse click by Internet user leaves electronic footprints generally without his/her notice. These electronic footprints contain efficacious means of information which provide knowledge of the sort of person that the user is and his/her interests. [6] On the internet sensitive information is gathered by credit card agencies, payment gateways, employers, income tax departments, service providers, advertsing agencies and social media. Use of cookies which gets installed on the hard drive of a user is fairly common in behavior. Some cookies may even communicate sensitive data about a user to an advertsising agency which may share this further with another line advertising agency without permission. This is a matter of serious concern at international level.

2. THREATS TO PRIVACY IN CYBER SPACE: A REFLECTION

[3] Robert S . Peck, *The Right to be Left Alone*, 15 Human Rights, 26-51 (Fall 1987).Published by : American Bar Association Stable URL : http://www.jstor.org/stable/27879466, 15 26–31 (2017).

[4] A typical KOOBFACE infection starts with a spam sent through Facebook, Twitter, MySpace, or other social networking sites. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-real-face-of-koobface.pdf(May 8, 2018, 12:18 PM)

[5]Ian C Ballon, E-Commerce and Internet Law, 6.01 2 (2011). http://www.ianballon.com/uploads/3/7/5/7/37570981/treatise_2017.pdf, (Dec.9, 2017, 3:45 PM).

[6] Francois Nawrot, Katarzyna Syska and Przemyslaw Switalski, *Horizontal application of Fundamental Rights – Right to Privacy on the Internet*, 9th Annual European Constitutionalism Seminar (May 2010), University of Warsaw,http://en.zpc.wpia.uw.edu.pl/wpcontent/uploads/2010/04/9_Horizontal_Application_of_Fundamental_Rights.pdf> (Dec. 19, 2017, 9:15 AM).

The word 'Cyberspace' was first used by William Gibson, in his book, Necromancer, written in 1984. Cyberspace can be defined as a virtual world of computers where internet is involved, where individuals can interact, conduct business, do transactions, and develop graphics.[7] In 1960s Internet was developed for better communication and research. With the advancement of 'e'- technology, everything becomes effortless to access as well as a pathway to commit crimes without any endeavour.[8] Nothing encapsulates the Web 2.0 concept more than social networking sites, which provide users the ability to connect, communicate, and share with others. However, recent years have seen a series of "moral panics" regarding information accessible on the Internet and its use for criminal activity.[9] Following are threats to cyber privacy:

2.1 Cyber Snooping: We see advertisements on the internet offering software that will let us monitor activity on a computer. These ads bark "Catch a Cheating Spouse" or "Secretly Monitor Email" or "Spy on Your Computer." In many circumstances, this type of software is not only sneaky, it's criminal.[10] Cyber Snoop trace Internet activity by looking at content as it passes to and from any computer via computer's built in Winsock program. This approach empowers Cyber Snoop to run reliably and mutely in the background. The only indication that Cyber Snoop is running is the manifestation of an optional cautioning message on the workstation. Cyber Snoop's configuration software permits to customize how we track and restraint accessibility to Internet Web, E-mail, Chat (IRC, AIM, ICQ, MSN, Yahoo! and Java™), News and FTP. Profiles are used to superintendence the Internet access of individual users. User names are assembled from system's available Windows User names. Without any doubt it infringes privacy.[11]

2.2 Corporate Espionage: The growing supercilious stakes game of corporate espionage is being played by individuals, corporations and countries worldwide. These players use any ethical, and in most cases, any unethical, means to obtain data that will give them a competitive or fiscal advantage over their rivalry. The level of seriousness and devotion

[7] http://www.williamgibsonbooks.com/books/neuromancer.asp (Oct. 4, 2017, 7:10 PM).
[8] K. Pandey, *Low Security makes Natives Vulnerable to Cybercrimes*, 2012, http://articles.timesofindia.indiatimes.com/ indore/31863717_1_cyber-crimes-cyber-cellcyber-criminals (4 Nov., 2017, 9:30 AM).
[9] Sean M. Zadig and Gurvirender Tejay, *Emerging Cybercrime Trends: Legal, Ethical, and Practical Issues*, http://www.irma-international.org/viewtitle/59936/> visited (Oct. 1, 2017, 10:45 AM).
[10] https://www.flashbackdata.com/when-snooping-becomes-a-crime/ visited on (May 8, 2018 3:11 PM).
[11] http://www.pearlsoftware.com/resources/snoopguide.pdf(May 7, 2018, 3:03 PM).

of these players for the game of corporate espionage is evident by the use of tools namely SCI-EAR 2000, SCI-MP1700 and SCI-DP4802 that tarnishes privacy of an individual. To gain superiority over their competitors, many corporations are hiring ex-military and government agents trained in the profession of spying -- I mean 'intelligence congregation techniques'. These skilled individuals are used to head new company divisions whose mission is to spy on and obtain information from competitors under the guise of competitive intelligence. [12]

2.3 Cyber Stalking: The Internet is a global medium regardless of boundaries and frontier that provides a pathway to Cyber-Stalker.[13] Cyber Stalking means to stalk someone by various modes like: (1) Following the posts of concerned persons, (2.) Noting down personal details i.e. contact details and address, (3) Favorite colour, (4) Favorite Food & Restaurant, (5) Downloading pictures, (6) Shopping Choices and (7) Friends List. This term is used interchangeably with online harassment and online abuse. Famous cases reported are Ritu Kohli [14] and Yogesh Pandurang Prabhu[15] where the offence was made against accused under section 509 IPC, Section 67, 67 A of the IT Act, 2000 (2008) and accused was punished in cyber stalking case.

2.4 Identity Theft: The word 'phishing' is commonly used to describe the offence of electronically impersonating someone else for financial gain. This is frequently done either by using someone else's login credentials to gain access to protected systems or by the unauthorized application of someone else's digital/ electronic signature in the course

[12] Eamon Javers, Secrets and Lies: The Rise of Corporate Espionage in a Global Economy, 12 Geo. J. Int'l Aff. 53, 60 (2011).

[13] Louise Ellison and Yaman Akdeniz, *Cyber-stalking: the Regulation of Harassment on the Internet*, http://www.cyber-rights.org/documents/stalking_article.pdf (Oct. 2, 2017, 7:05 AM).

[14] The Delhi Police registered India's First Case of Cyber stalking. One Mrs. Ritu Kohli complained to the police against one who was using her identity to gossip over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days. Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking in unchaste language. The same person was also deliberately giving her telephone number to other chatters inspiriting them to call Ritu Kohli at odd hours. Consequently, Mrs Kohli received almost 40 calls in three days mostly at odd hours from as far away as Kuwait, Cochin, Bombay and Ahmadabad. The said calls created havoc in the personal life and mental harmony of Ritu Kohli who decided to report the matter. http://www.informaticsjournals.com/index.php/gjeis/article/viewFile/3059/2143 (Oct. 4, 2017, 1:02 AM).

[15] The State (Cyber Cell) vs. Yogisha @Yogesh Pandurang Prabhu, 2015.

of electronic contracts. Increasingly a new type of crime has emerged wherein sim cards of mobile phones have been ‘cloned’ enabling miscreants to make calls on others' accounts. This is also a form of identity theft. Two sections of the amended IT Act penalize these crimes: Section 66C makes it an offence to “fraudulently or dishonestly” make use of the electronic signature, password or other unique identification feature of any person. Similarly, section 66D makes it an offence to “cheat by personation” by means of any ‘communication device’ or 'computer resource'. Both offences are punishable by imprisonment of up to three years or with a fine of up to Rs. one lakh.

2.5 Vishing: As indicated by the word ‘Vishing’- this has come from “voice,” and “phishing”. Vishing is the act of using the telephone in an attempt to scam the user. Much the same as 'phishing' is the utilization of caricature messages intended to trap focuses on clicking malevolent connections. Rather than email, vishing, for the most part, depends on robotized telephone calls, which teach focuses to give account numbers to the motivation behind money related reward. Vishing Scams work: Criminals set up a mechanized dialling framework to the content or call individuals in a specific district or region code (or in some cases, they utilize stolen client telephone numbers from banks or credit unions). The casualties get messages like: "There's an issue with your record," or "Your ATM card should be reactivated," and are coordinated to a telephone number or site requesting individual data. Some of the time criminal statement some data about your record before requesting that you enter data, with the goal that anybody could trust it's a validated source. [16] By and by, many instances of this nature are going on in daily papers.

2.6 Website Defacement*:* Website defacement is novice offence against websites with an intention to cheat innocent visitors of the website. It is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own. Defacement is generally meant as a kind of electronic graffiti and, as other forms of vandalism, is also used to spread messages by politically motivated "cyber protesters" or hacktivists. It is the more improved concept of Pharming.

[16] https://www.cnet.com/news/protecting-yourself-from-vishing-attacks/ (Oct. 4, 2017, 12:05 AM).

2.7 Copyright Infringement: Copyright is a legal right granted by the government to the authors or creators of works. Under the copyright law, the copyright owner is entitled to a number of exclusive rights such as the right to publish the work, control copying, and prepare derivative works and the right to make the material available online. Copyright protection becomes applicable immediately upon creation of the manuscript. The Indian Copyright Act, 1957 governs and regulates the system of copyright in India, however, maximum of the copyright violations occur on the Internet like Clicking, Downloading pictures without consent and uploading on the Internet.[17]

3. INDIAN LEGAL PROVISIONS ON THE PROTECTION OF PRIVACY IN CYBER SPACE: AN ANALYSIS

Privacy itself seldom involves attempts to cloak one's actions from public scrutiny. Privacy is merely a demand that the requirements for public security and individual accountability not spill over into otherwise unreasobable intrusions into one's personal beleifs and activities that have no relavance for the public. It is not easy to define the ambit of 'Privacy'. It is also coined as- "the right to be left alone" by Warren and Brand is in their seminal law review article of nearly a century ago. Privacy is another name for personal autonomy, a notion that captures the various libertarian strains that also equate freedom with personal sovereignty. As Oliver Wendell Holmes declared it as "the life of the law has not been logic: it has been experiencing."[18] Privacy was a theme that had great appeal to Louis Brandeis. In an often quoted dissent in Olmstead v. the United States (1928)[19], the significance of which was later recognized, Justice Brandeis wrote:

[17] The Copyright Act, 1957 has been amended four times so far in 1983, 1984, 1992 and 1999. http://vle.du.ac.in/file.php/697/Cyber_Crimes_Cyber_Security_and_Legal_Aspects/Introduction_to_Cyber_Crimes_Cyber_Security.pdf, (Jan. 4, 2018, 4:00 PM).

[18] In 1890, Louis Brandeis, and his law partner Samuel Warren wrote the most famous article on the right to privacy in American history. Warren and his young wife, Mabel, were upset about gossip items in the Boston society press — including stories about Mrs. Warren's friendship with President Grover Cleveland's young bride — and this aristocratic distaste for invasions of what Warren called their "social privacy" led him to seek Brandeis's help in proposing a new legal remedy. https://www.washingtonpost.com/opinions/clash-between-free-speech-and-privacy-in-the-digital-world/2015/03/20/bee390e6-c0f8-11e4-ad5c-3b8ce89f1b89_story.html?utm_term=.b26b05f931c5, (Dec. 9, 2017, 7:19 PM).

[19] 277 U.S. 438 (1928).

"The makers of our Constitution undertook to secure conditions favourable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect... they conferred, as against the Government, the right to be let alone- the most comprehensive of rights and the right most valued by civilized men."

Unlike the European Union, India does not have any separate law which is designed exclusively for the data protection. However, the courts on several occasions have interpreted "data protection" within the ambits of "Right to Privacy" as implicit in Article 19 and 21 of the Constitution of India. However, the Ministry of Electronics and Information Technology has appointed an expert group headed by former Supreme Court judge BN Srikrishna to draft a data protection law.[20]

Just as the right of privacy is not absolute even in one's home, similarly this right outside the home is also not absolute. As one moves from the private realm to a more public one, it naturally follows that his or her expectation of privacy is reduced. Indeed, the courts, in attempting to apply the right of privacy, have placed substantial emphasis on a balancing the right to privacy.[21]

1. ***The Constitution of India, 1950***: Indian Indian jurisprudence, does not provide an express definition of the 'right to privacy' however, the same could be derived from right to personal liberty under Article 21.[22] Right to privacy is not an absolute right, for it is a corollary of Article 19(1) (a) and Article 19(1) (d) alongside Article 21.[23] Recently, the judgment of Justice K S Puttaswamy (Retd.) versus the Union of India delivered on 24 August 2017 by Supreme Court has made it a historic day as it has crowned Indian Constitution with another jewel namely: 'Fundamental Right to Privacy'.
2. ***The Information Technology Act, 2000 as amended in 2008: Relevant Provisions***

The Information Technology Act was enacted in 2000 and has been revised most recently 2008. The Information Technology (Amendment) Act, 2008 has added several provisions that are privacy-centric. Sections 43 deals with Penalty and Compensation for damage to computer,

[20] http://www.news18.com/news/india/right-to-privacy-data-protection-laws-in-india-1500047.html (Dec. 24, 2017, 8:29 AM).
[21] Robert S. Peck, *The Right to be Left Alone*, American Bar Association, Stable URL : http://www.jstor.org/stable/27879466, 15 26–31 (2017).
[22] For more details see: Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[23] For more details see: Govind v. State of Madhya Pradesh & Anr, 1975 AIR 1378. Held that: The right to privacy is subject to restrictions, akin to other partial rights, on the basis of compelling public interest.

computer system, Section 66 deals with computer related offences, Section 66-C deals with Identity Theft or Hacking, Section 66 D provides punishment for Cheating by Personation by using computer source, Section 66 E deals with punishment for violation of privacy, Section 67 C provides Preservation and Retention of information by intermediaries, Section 69 states powers to issue directions for interception or monitoring or decryption of any information through any computer resource, Section 72 mentions regarding privacy and confidentiality and Section 72 A deals with Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008) of the Information Technology Act, 2000, which relate to computer/cybercrimes. The Act is lacking in many ways, including: (1) No definition of "sensitive personal data" is clearly defined. (2) The IT Act is silent on Cyber privacy issues. (3) The IT Act makes hacking and tampering with computer source an offence and penalizes unlawful access to data. However, does not prescribe any minimum security standards which the entities having control of data should comply with except in cases of Personal sensitive information.[24]

3. The Data (Privacy and Protection) Bill 2017 & 2019:

The Justice BN Shrikrishna Committee was formed to propose a draft data protection regime to identify current issues and possible statutory protections. The Data (Privacy and Protection) Bill, 2017 and 2019, grants a statutory Right to Privacy. The Bill also proposes to streamline the data protection regime in India by providing a holistic framework and proposes the creation of the Data Privacy.[25] This Bill has discussed several emerging privacy issues, 'legitimate expectations', BHIM (Bharat Interface for Money), 'due diligence', 'consent criterion' and online banking.

4. CONCLUSION AND SUGGESTIONS

Around the globe, cybersecurity has taken a new urgency as the digital economy has matured over the past decade. Moreover, the importance of cybersecurity endures to expand each day with the emergence of a modern wave of cyber-physical systems that constitute up the 'Internet

[24] http://www.livelaw.in/data-protection-india/ (Jan. 3, 2018, 1:00 AM).

[25] http://www.livelaw.in/relevance-data-privacy-and-protection-bill-2017-highlights-entails/ (Jan. 1, 2018, 5:42 PM).

of Things'; that embrace wearables, "smart" devices for the home, autonomous vehicles, and unmanned aerial systems (also known as drones). Yet against this backdrop of digital metamorphosis, it is increasingly clear that both the public and private sector are failing to keep pace with cybersecurity threats.

There are three cardinal sectors of vulnerability in any nation's cyber realm: (1) Government and Military; (2) Industrial & Economic; and (3) Individual users in the civilian or private sector, who may reciprocate in myriad ways with either of the two foregoing sectors, as well as with each other. [26] Presently the greatest persistent vulnerability is with individual users who fall prey in the hands of cyber criminals because of sharing their information. The benefit of anonymity goes to the wrong doers. However, in the recent case Independent Newspaper Inc. vs. Brodie[27] that was filed by a model Liskula Cohen whose photograph was on the cover page of 'Vogue' wherein was defamed as "Shankiest in NYC' on a blog. the court of Maryland ordered Google to disclose the identity of the anonymous person who had posted the comment.

The author observes that 'Cyber Privacy' means, "Desire of every individual for virtual space where one can be free of interruption and intrusion of personal information". It is submitted that 'Privacy' is a myth in the complex web of websites unless and until netizens (users in cyberspace) are techno-experts. Presently, Machines are used to deal with Machines and Software are used to ensure privacy in the virtual world. Advanced settings and Applications are utilized against unauthorized intrusion. However, Cyber Jurisprudence must not be a mute spectator. It is ripe time to absorb features of technology and strengthen legal domain with techno-legal provisions. In addition to these, stringent legal provisions must be enacted to protect data in the virtual world. Some of the suggestions are submitted as follows:

1. The essence of cyber privacy lies in 'Awareness' and 'Selection of Information' to be shared by each individual on online platform.
2. Need to inculcate cyber ethics. Cyber ethics means the field of inquiry dealing with ethical problems aggravated, transformed or created by computer and network technology.[28]

[26] George R. Jr. Lucas, Privacy, Anonymity, and Cyber Security, 5 Amsterdam L.F. 107 (2013).
[27] 966 A. 2d 432 (Md. 2009).
[28] https://www.albany.edu/~goel/classes/spring2006/workshop/cyberethics.pdf (May 8, 2018 1:55 PM).

3. Law strategies must include a comprehensive compliance process, management of internal privacy, employee training, awareness, self-regulatory efforts, corporate interface with privacy awareness seminars and online dispute resolution mechanism. Every corporate, private, as well as government sector, must comply ISO/ IEC: 27001: [29] Information Security Management standards.
4. The internet service providers must strictly verify, upon an individual's connection or 'handshake' with the provider[30], that the individual user has installed. With this an unsafe or unsecured individual user would not be permitted public access to the 'information superhighway', just as an unsafe vehicle would be prohibited from driving on public thoroughfares.

[29] The ISO/IEC 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS), https://www.iso.org/isoiec-27001-information-security.html (Jan. 5, 2018, 8:53 PM).

[30] George R. Jr. Lucas, Privacy, Anonymity, and Cyber Security, 5 Amsterdam L.F. 107, 114 (2013).