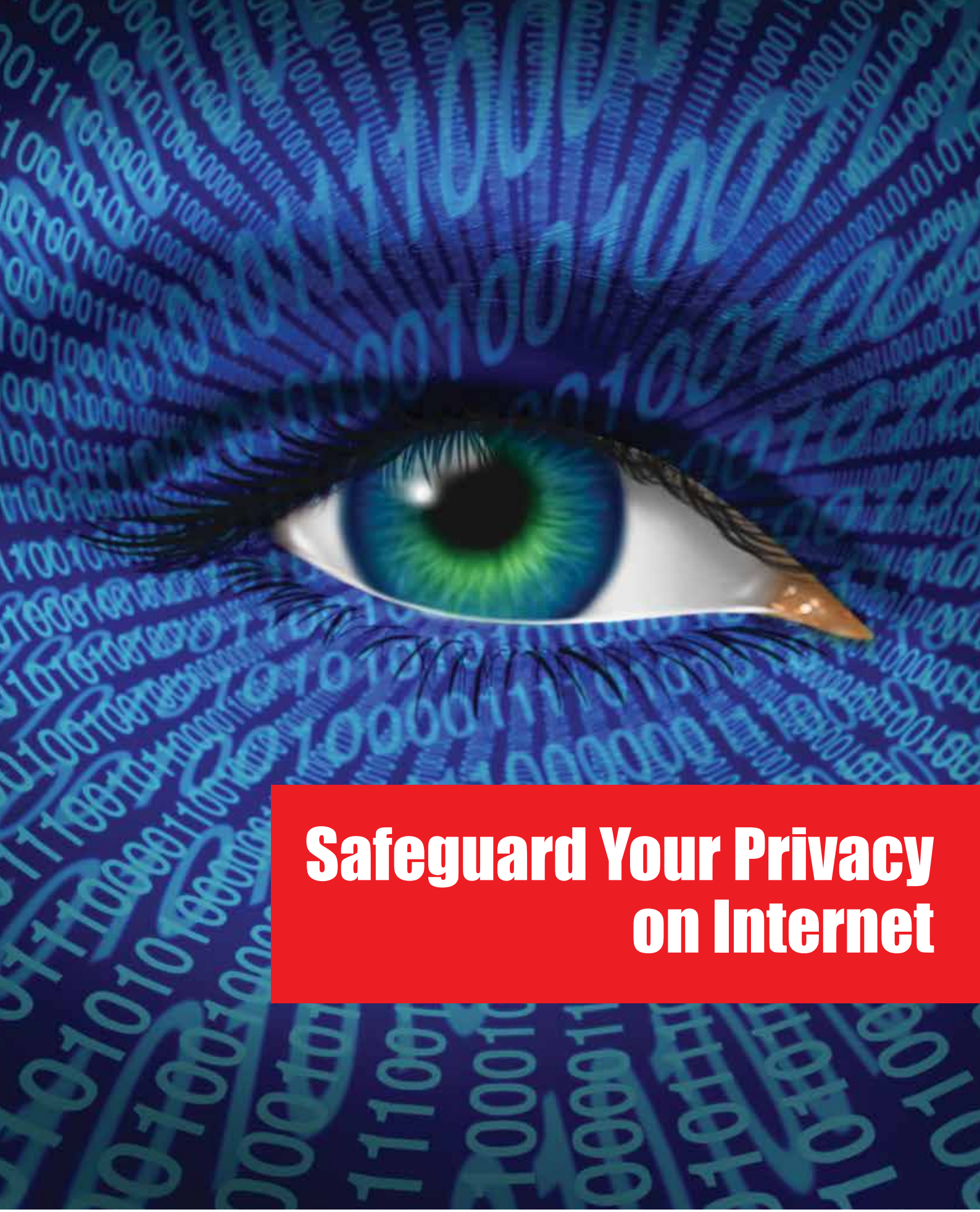

Safeguard Your Privacy on Internet

Karnika Seth

OakBridge

Preface

In today's digital times, the notion and concept of Privacy has transformed and evolved in a revolutionary pace! We all freely share personal information with friends and relatives on social media and give away personal information while registering for e-services or purchasing goods online. Use of cookies has made behavioral advertising a powerful marketing technique of online retailers. Some common questions emerge, what data do we really need to share? How will this data be used? Can it be misused? What is privacy? How can it be protected? How does Privacy ruling of none judge bench impact us? Can government put restrictions on our right to privacy? What is the law on Privacy in India? What can we do to safeguard our Privacy online? This is precisely the reason for writing this e-book . It is meant to be an easy guide for students, law students, professionals, lawyers, infact it caters to all netizens to understand how we can protect our privacy online. The book also aims to give a brief overview of how Privacy is Protected in U.S and Europe and recent changes in law. I hope the readers find the e-book interesting, educative and useful to improve online safety!

For any questions or comments, please feel free to contact me.

Karnika Seth
karnika@sethassociates.com
linked in-- https://www.linkedin.com/in/karnika-seth-1100873/
twitter- https://twitter.com/karnikaseth
http://www.karnikaseth.com
freeapp-IT Act,2000 & Cyberlaw India
https://play.google.com/store/apps/details?id=com.sethassociates.com&hl=en
You tube channel-https://www.youtube.com/channel/UCGpGgvHDdglgawxO7-4bwng

About The Author

Karnika Seth is an internationally renowned Cyber law expert & the Founder Partner at Seth Associates law firm in India. Ms Seth is also the Chairperson of Lex Cyberia at Seth Associates, the World's first integrated cyber laws research, forensics and legal consulting centre. Ms. Seth has been consistently ranked by global business community as distinguished cyber lawyer, an IT Expert & a prolific Author & Educator. Her contribution to growth & development of cyber laws and spreading its awareness internationally and in India is widely acknowledged in the corporate world and by International organisations. She contributes to various Working Group Consultations and ICANN discussion forums aimed at designing policies for Next Generation Internet. In 2013, she was appointed as legal expert to represent Indian Government to advise on objections to ICANN's suggested new gTLDs. She is part of Expert Panel of UNICEF working on children safety in the online world and actively associates with International Centre for Missing and Exploited Children (ICMEC) in its Think Tanks & cyber awareness activities in India. She is also associated with the International Telecommunication Union's initiatives and is a member of the Global Cyber Security Forum. Her expert views on cyber safety have been solicited by Indian Parliament and the Ministry of Information Technology for strengthening cyberlaws in India. She is empanelled as legal expert to advise National Internet Exchange of India, National Commission of Child Rights and the Office of Comptroller of Certifying Authorities constituted under the IT Act, 2000. She is member of Advisory Boards of various educational institutions and was conferred title of Honorary Professor by Amity University in 2017.

Ms. Seth practices law at the Supreme Court of India and is principal legal advisor to many multinational groups and government entities. She has actively resolved complex Cyber crime cases in conjunction with the law enforcement authorities in India. She is also an Expert IT law Educator & Trainer to law enforcement authorities in India including the National Judicial and Police Academy, Central Bureau of Investigations and The National Investigation Agency.

Ms. Seth writes extensively on key legal and cyber awareness issues for newspapers, journals and periodicals from time to time. Ms. Seth's book titled 'Computers, Internet and New Technology Laws' published by Lexis Nexis Butterworths elucidates the key developments in the field of Cyber laws across many important jurisdictions, India, United States and European nations. Ms. Seth was conferred the Law Day Award from the Chief Justice of India for authoring the comprehensive reference book in 2012. She received the Digital Empowerment Award for the year 2015 and the Law Day Award in 2015 for authoring the book, Protection of Children on Internet. Ms. Seth regularly contributes her views on the subject in conferences, print & electronic media and television.

SAFEGUARD YOUR PRIVACY ON INTERNET

By

Karnika Seth

Table of Contents

Introduction

The recent nine judge bench of the Hon'ble Supreme Court of India in *Justice K.S Puttaswamy v UOI & Ors*[1] passed a landmark ruling declaring the Right to Privacy is a Fundamental Right of every citizen of the country! The Apex Court ruled that Right to Privacy is intrinsic to life and liberty and stands covered by Article 21 of the Constitution of India. In today's world of internet and computers where we share information about our business and social life through social networks like LinkedIn and Facebook, the question arises whether the concept of Privacy is realized and respected by netizens. It is our conscious decision – what to share and how much to share and with which groups we associate with. The information we share could be of diverse nature, business or personal, as such client contacts, vendor information, affiliations, or pictures, ideas and thoughts in our business or social circle. We do value our privacy because there is certain amount of information we would like to keep personal. But the boundaries will vary for every individual. For this reason, it is advisable to read the terms and conditions of any web service before we subscribe to that service or download any application. It is mandatory for every website operating in India to declare the terms of use and privacy policy on its website as per the IT (Intermediaries Guidelines) Rules, 2011. The Author aims to share some useful insights into the concept of Privacy, through the interpretation of the recent nine judge ruling on Privacy and with few easy tips on safeguarding one's personal information online.

Definition of privacy

The right to privacy can be defined as 'the right of a person to enjoy his own personal space and his boundaries, physical, mental and emotional interaction with other individuals'. This right is said to have originated from an essay written by Warren and Brandeis, titled 'The Right to Privacy' which stated that the object of privacy is to protect 'inviolate personality'. The essay was published in 1890.[2] This right to privacy is examined from two quarters, one vis-à-vis other individuals and secondly the constitutional right against the state. On one hand a person may choose to limit his interaction with others. But on the other hand the government authorities may have special powers to conduct surveillance or intercept on electronic communications. This right to privacy is usually equated with one's right to property/ ownership[3]. In the European Union, the European Union Data Protection Directive, 1998 enshrines the privacy rights which are elucidated by Article 8 of European Convention of Human Rights. The universal declaration of Human Rights, 1948 also recognize the right to one's privacy. Similarly the International Covenant on Civil and Political Rules, 1996 grants recognition to right to privacy. This right applies equally in the virtual world. In India the right to privacy is protected by Article 21 of the Constitution of India that guarantees the freedom of life and personal liberty to all persons which has now been declared as a fundamental right in itself by the recent nine judge ruling of the Supreme Court of India in *Justice K.S Puttaswamy v UOI & Ors.* Similarly, in United States this right is considered fundamental under the first, third, fourth, fifth and ninth amendments.

[1]Writ Petition (Civil) No 494 of 2012
[2]Warren and Brandeis, the right to privacy, Harvard Lawrie View, Vol-4, No.5, 5th December,1890 pp 193-220.
[3]Millar, Arthur, *the assault of privacy, computers and data banks, Dossiers*, Arbor University of Michigan Press, 1971, pp211.

Risks to privacy on the internet

When we use the internet or computers, smart phones and other such devices, our location can be easily tracked. We voluntarily give away a lot of information about our self while registering with applications, or browsing websites including our hobbies, interests and videos one likes to watch. This puts one at risk as there are many cyber criminals on the world wide web, many of whom use the Dark Web[4]. Cyber criminals often use the malware such as key-logger that steal personal information after invading a system. One such incident is that of 'Koob Face', a malicious program which steals personal information of Facebook users to sell it to make wrongful gains. Cyber criminals often misuse information available on the internet to commit crimes such as Data Thefts, Corporate Espionage, Identity Theft and other crimes such as defamation, kidnapping or even murder. One such incident took place when a Mumbai based teenager, Adnan Patrawala, son of a businessman was trapped by an imposter on Orkut Social Network and was later murdered.

Why to read terms of use and privacy policy

Websites have adopted the technique of behavioral advertising as they watch the products and services you are interested in their website. They use cookies which get installed on the hard drive of a user. Each time you visit the same website, it recognizes you and starts popping the advertisements which may be of interest to you. Some cookies may even reveal sensitive data user to another Advertising Agency. Super Cookies are difficult to detect and delete from one's systems. Certain Networking sites such as Facebook have been reported to share information about its users to Advertising Agencies when seeking permission.[5] Similarly Version 5 of HTML Code has also been reported to provide to Advertising companies users' contents including location, time, photos, emails and web history.[6] Use of web bugs is also quite common today. It checks when a particular message or a web site is accessed by a user and saves its IP address. Whenever a company uses any such technique or mechanism to collect personal or private information about a user, it is required by law (applicable to most jurisdictions) to declare the same through its terms of use and privacy policy. In Amazon.com's case class action law suits were filed against an Amazon's subsidiary, Alexa Internet, alleging that it collected un-authorized user information including the use of credit cards by its users. Alexa was directed to pay US $40 to every affected party whose personal sensitive data was compromised. In India, in a petition, the action of WhatsApp sharing personal data of users with Facebook and other parties as alleged to violate the privacy of users of WhatsApp. The case is pending before the Apex Court[7]. Recently, India has also set up an expert Committee under chairmanship of Justice B.N Srikrishna to draft a data protection law, which will ensure data collected from persons is collected, processed and used in a fair and reasonable manner and lay down the right parameters in law so that it does not violate privacy of any person\\.

[4]Dark Web is that part of the web wherein persons may use the software to conceal one's true identity through hiding the real IP address. Such activity is also misused by criminals to carry out illegal activities as selling drugs or child pornography.

[5]Brad Stone, *How Face Books as well as your friends, Bloomerang "Business Week", 24th September,2010.*

[6]Version 5 on web got misspelled and/or privacy, the Times of India, 12th October,2010.

[7]Express News Service, "Supreme Court to Facebook, WhatsApp: Have you shared user details?", Indian Express, http://indianexpress.com/article/india/supreme-court-to-facebook-whatsapp-have-you-shared-user-details-4832144/

The IT (Intermediary Guidelines) Rules, 2011 mandatorily require websites to declare its privacy policy and terms of use on its website. It is therefore very important to read the privacy policy and check what data will be collected from the users, and how it will be shared, including when an organization is acquired by another company, for example, the WhatsApp and Facebook controversy. When availing service from a website a user can opt out when it is asked for permission to collect personal data. In India this opt out option is provided in Rule 5 of Information Technology (Reasonable Security Practice and Procedure and Sensitive Personal Data or Information) Rules, 2011. This requires every corporate that collects sensitive personal information of an user to obtain written permission for its collection and disclose purpose of its use. Rules also allow the user to withdraw the consent which may have been given earlier by him or her. At the Consumer Level Technical Standard such as P3P programs are incorporated in the browsers which restrict the information about the user, collected while surfing the internet. It is advisable to use good anti-virus and good anti-spyware to block any online virus attacks. For the safety of children, child accounts can be installed in smart phone or laptops with filters/ restrictions on content browsed or downloaded/ uploaded from a child's device.

What is sensitive personal information?

In India, Section 3 of the IT (Reasonable Security Practices and Procedure) Rules, 2011 explains 'what is sensitive personal information?' It means personal information, which comprise of one's password, financial information such as bank account, credit card or physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information given to a body corporate to process, store any such information under a lawful contract or otherwise. According to Section 43A of the Information Technology Act, any body corporate that collects personal sensitive information about a person, ought to maintain reasonable security practices in order to secure the information. Failure to do so makes them liable to compensate the aggrieved party and such cases are decided by the Adjudicating Authority appointed under Section 46 of the Information Technology Act. It is also important to note that Sections 72 and 72A of the IT Act, 2000 makes unauthorized disclosure or use of personal sensitive information by a person who is authorized to perform functions under the IT Act or by a private service provider (respectively) an offence under the Act, and it amounts to breach of confidentiality and privacy of a user. Such person can sue the offender for compensation before the Adjudicating Authority appointed under Section 46 of the IT Act. According to Section 72, such person is liable for breach of confidentiality for a punishment of two years or fine upto Rs.1.00 Lac or both and according to section 72A such service provider is liable for punishment with imprisonment for a term upto three years or fine which may extent to Rs.5.00 Lacs or both.

Indian Case Laws on protecting privacy

The nine judge ruling of the Supreme Court of India upheld Right to Privacy as a Fundamental Right of every person of the country. In its 547 pager judgement that declares privacy to be a fundamental right, the Supreme Court overruled the verdicts given in the *M.P. Sharma* case in 1958 and the *Kharak Singh* case in 1961, which earlier held that the right to privacy is not protected under the Indian Constitution. However, this is not an absolute right and can be curtailed by a

procedure established by law which is fair, just and reasonable. The Hon'ble Supreme Court of India in *Kharak Singh v. State of U.P.*[8] held that the Domiciliary visits to a suspected place at night is violative of Article 21 of the Constitution and struck down the provision, Regulation 236 of U.P. Policy Regulations as unconstitutional. In another case, *Govind v. State of U.P.*[9] the Court upheld the right to privacy and held that it can be restricted only in accordance with the procedure prescribed by law. In *A. Raja v. P. Srinivasan,*[10] the court granted interim injunction to restrain the defendant who was a publisher of a weekly magazine from publishing pictures of plaintiff's wife and children along with the allegations against the plaintiff to be a corrupt Public Officer on the ground that it violated plaintiff's privacy. In *Shashank Sekhar Mishra v. Ajay Gupta*[11] the Delhi High Court restrained the defendant in a suit for permanent injunction from disclosing private information pertaining to the plaintiffs and his family and using his software. The Court took the view that even public authorities are not entitled to invade a person's privacy in India except in accordance with law. In an interesting case before the Delhi High Court the issue involved extending the right to privacy to include right to be forgotten[12]. The petitioner sought that he be "delinked" from information regarding a criminal case involving his wife where he was not a party. The Court directed the defendant's websites to remove the specific results for queries which include his name in the Database.

Legal provisions protecting Privacy under Indian Information Technology Act, 2000

Under Section 66E of the IT Act, 2000 the offence of Video Voyeurism is prohibited.

According to Section 66E, any person who intentionally or knowingly captures, publishes

[8]1964(1) SCR332
[9](1975) SCC(CRI) 468
[10]2009(8) MLJ 513
[11]2011 (184) DLT 675
[12]http://www.livelaw.in/delhi-hc-hearing-nris-plea-right-forgotten-read-petition

or transmits the image of private area of any person without his/her consent that violates the privacy of that person, shall be punishable with imprisonment which may extend to three years or fine upto Rs.2.00 Lacs or both.

Section 72 of the IT Act prohibits disclosure of personal information of a person received by a person in his official capacity under the IT Act, 2000. A person who breaches section 72 is liable for imprisonment for a term upto two years, or fine upto Rs.1.00 Lac, or both. However any information disclosed to another Law Enforcement Authority shall not be considered a breach of section 72. Section 72A of the IT Act, 2000 puts a similar obligation on a private service provider such as internet service provider.

Section 67 prohibits publishing or transmitting of pornographic material in electronic form. Section 67A prohibits publishing or transmitting any material containing sexual explicit act in electronic form and section 67B prohibits child pornography. While the punishment for violation of section 67A is upto five years of imprisonment and fine upto Rs.10 Lacs, and for second subsequent conviction with imprisonment of a term upto seven years and fine upto Rs.10 Lacs, violation of section 67B provides for a punishment of imprisonment upto five years and fine upto Rs.10 Lacs.

Section 66 prohibits computer related offences including unauthorized copying for access of data or damage to a computer data base and

destruction or deletion or alteration of any information residing in a computer resource or diminishing its value or utility. Violation of Section 66 is punishable with imprisonment for a term upto three years or fine upto Rs.5.00 Lacs or both. Section 43 is attracted where there has been a contravention but no mala-fide intention was there to commit such an act. It is similar to a tort and makes a person liable for payment of compensation to the affected party. Section 43A of the IT Act obligates a body corporate to compensate the affected party whose personal data has been disclosed without permission or consent leading to wrongful loss caused to such person or the wrongful gain to any person. There is no limit to the amount of compensATION THAT CAN BE CLaimed under this section.

Snooping by spouse

As a practicing cyber lawyer too, the Author has seen a steep rise in the number of cases using electronic evidence particularly in cases involving domestic violence, cruelty, filed by a spouse before Indian Courts and abroad. In most cases, a party would use audio recorded private conversation which are unauthorizedly recorded. In many cases email accounts /social media accounts of a person is hacked by his/her spouse and is produced as evidence to prove adultery or other similar allegations of matrimonial infidelity. Such cases are a direct attack on one's *right to privacy. In an important decision, Rayala M Bhubaneswari v. Naga Phanender Rayala,*[13] the husband unauthorisedly recorded a telephonic conversation of his wife when she was speaking with her relatives and produced it in evidence in a divorce proceedings. The Andhra Pradesh High Court upheld one's right to privacy and held as follows:

> *"….There should be some trust between husband and wife and in any case, in my view, the right of privacy of the wife is infringed by her husband by recording her conversation on telephone to others and if such a right is violated, which is not only unconstitutional, but also immoral, later on, rely on the evidence gathered by him by such means. Clearly, it must not be permitted."*

In many cases, a party would rely on illegally obtained log data of phone calls of his or her spouse to support the case. After the ruling of the nine judge bench, the Right to privacy became a fundamental right, and a spouse will certainly have a cause of action against the other spouse if such data has been unauthorisedly gathered and produced before a Court of law. A party that comes to Court, even otherwise must come with clean hands!

Privacy rights of employees

Subject of employees' surveillance is still evolving in India. The level of surveillance that an employer is permitted to carry out depends on the organization's HR policy and information technology policy. CCTVs, email, monitoring tools are most commonly used techniques for surveillance. However, although official email accounts of employees can be monitored, the personal email accounts of employees generally cannot be monitored. In European Union, the general EU directives on personal data protection apply to employees with regard to processing of personal data and free movement of such data. Certain States such as Massachusetts have framed regulations which require business entity that owns, licenses or stores personal information of its residents to use a written comprehensive

[13] AIR 2008 AP 98

information to safeguard this information.[14] In India, the contract law will determine if the surveillance measures are satisfied or void against public policy and if they violate an employee's Right to Privacy.

Privacy protection vis-à-vis government

Although Article 21 of the Constitution of India guarantees right to privacy as a part of fundamental right to life and personal liberty, the same is not an absolute right and will be subject to reasonable restrictions that may be placed on the said right. These restrictions will however be as per procedure established by law. The government has right of interception of electronic communications and surveillance of traffic data. In India, Section 69 of the IT Act, 2000 empowers the central government or the state government to issue directions for interception, monitoring or decryption of any information through any computer resource in order to protect sovereignty or integrity of India, defense of India, security of state, friendly relation with Federal States or public order or preventing incitement to commission of any cognizable offence or investigation of any offence. Section 69A of the IT Act, 2000 empowers the central government to issue directions for blocking public access of any information through a computer resource. Similarly, Section 69B empowers the central government to monitor and collect traffic data or information through any computer. The central government has passed the IT (Procedure and Safeguard for inception, monitoring and decryption of information) Rules, 2009 to lay down the frame work and legal process for such interception. Such interception requires authorization from the Secretary of the ministry of home affairs, central government or state government. But in emergency such interception could be even issued by an officer not below the rank of Joint Secretary to the Government of India. The sensitive data collected is required to be maintained by the security agency and should be destroyed after six months, unless it is needed for further investigation. Such data is kept confidential by all means. It is pertinent to mention here that India's central monitoring system gives law enforcement agencies centralized access to India's Telecom Network with facility to record ordinary calls, VOIP calls, chat and locate a person's location. Its headquarters are in Delhi and it has 22 monitoring centers. The IT (Procedure and Safeguards after monitoring and collecting traffic data or information) Rules, 2009 were passed to allow monitoring of traffic data after the Secretary, Ministry of IT approves such monitoring. Rule 5 of the said Rules puts the intermediaries under an obligation to maintain confidentiality of such monitoring activity. Such right to interception of electronic communications is also seen in other countries such as United States of America. In United States, under the Communication Associations for Law Enforcement Act phone calls and internet traffic is required to be made available for uninterrupted real time monitoring by Federal Law Enforcement Agencies. In 2007, German Federal Police launched 'Bundestrojaner' project but the Federal Constitutional Code struck down the surveillance holding that Trojanzing the computer of a suspect is constitutionally permissible only if actual evidence of concrete danger exists and can be undertaken only with judicial authorization. An interesting question arose concerning privacy rights, where identity of a blogger can be revealed where a post is put anonymously. In a recent case, a model named, Liskula Cohen whose photograph was on the

[14] 201 MASS Code REGS 17

vogue magazine was defamed as "Skankiest in NYC" on a blog. The court ordered google to disclose the identity of the anonymous person who posted the comment.

In another case, *Independent Newspaper Inc v. Brodie,*[15] the Court of Appeals of Maryland laid down the 5 point tests for disclosure of the identity of a forum member while dealing with a defamation suit. The test included criteria such as defamation giving reasonable notice to the anonymous person, giving such person time to oppose disclosure, specifically the defamatory statements alleged to be made and proving a prima facie case of defamation and proving the balance of convenience lies in favour of disclosure of his identity. In India, the police is empowered under section 91 of the Criminal Procedure Code to identify a person who has committed an illegal activity and obtain his phone related information and details of his email/social media account.

Further, in India, the Right to Information Act, 2005 entitles a person to seek information from public authority. According to section 8(1)(j) of Act disclosure of such information that could breach a person's privacy is an exception and thus stands protected. In *Secretary General, Supreme Court V. Subhash Chander Agarwal,*[16] the court held that a fine balancing of requirement is needed to protect one's right to information vis-à-vis right to protect privacy between government entities and individuals.

International organizations protecting privacy

A number of international organizations such as the Organization for Economic Cooperation and Development have issued model guidelines to protect privacy. The privacy guidelines,1980 is one such instrument. APEC (Asia Pacific Economic Cooperation) also formed a privacy policy in 1994 to protect personal information from unauthorized transactions. Similarly, European directives on privacy data protection provides the parameters to be satisfied in order to protect personal information. The Council of Europe passed the Internet privacy guidelines for Internet users and service providers. In 1995 European Union passed the data protection directive to protect data of individuals within the European Union. Recently the General Data

[15]966A2d432 (Md 2009)
[16]AIR 2010 DEL159

Protection Regulation (GDPR) was formed by which the European Parliament, the Council Of European Union and the European Commission intend to strengthen and unify principles which formed a part of this guidelines and purpose within data protection for all individuals within the European Union (EU). It also regulates the transfer of personal information of European citizens outside India. The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period. It will replace the Data Protection Directive, 1995. The underlying principles in most regulations / softcode on privacy have following parameters-

Requirement of Prior notice and express consent

(1) This means that in order to collect any data from any individual such person must be given prior notice of information which is sought to be collected. Such person may accept or reject such a request in clear terms.

(2) **Legitimacy of purpose:**
The data collected for a legitimate purpose and only to the extent required to satisfy the object of collection.

(3) **Use and disclosure restrictions:**
The information collected can be used for only the specified purposes i.e. authorized and not disclosed or used for other purpose.

(4) **Time period for retention:**
The information collected is only to be retained for such time as is required to meet the objectives of collection.

(5) **Right to update information of any individual:**
Right to update one's information and the party that requires such information should maintain its accuracy.

(6) **Right to access information:**
Every individual has the right to check the information that is collected about him and its information should be kept confidential.

Changes in privacy law in EU

In U.S, the Electronic Communication Privacy Act bans unauthorized access to a computer network and provides steps that government must follow to seek information about a user from an Internet Service Provider. ECPA empowers the government to freeze the records of electronic communications pursuant to 18 USC Section 2703(f). In India, the law of interception is provided in the Telegraph Act and the Rules formed under the I.T. Act, 2000. The real time electronic surveillance in criminal matters is governed by Wiretap Statute, 18 USC Sections 2510-2522 and the pen/trap statute, 18USC Section 3121-3127. Few important legislation pertaining to privacy and data protection in the USA include the Computer Fraud and Abuse Act, Children Online Privacy Protection Act, 1998, Video Privacy Protection Act, 1998, Sarbanes and Oxley Act, 2002, Gramm and Leach Bliley Act, Fair Credit Reporting Act, Health Insurance Probability and Accountability Act,1996. In

European Union, the GDPR Regulation will unify the rules that govern data privacy of citizen sin the EU. Unlike a directive, it will not need nation specific legislation to protect data of its citizens. In UK Article 5 of the General Data Protection Regulation requires –

- Personal Data should be processed fairly, lawfully, and in a transparent manner;
- Collected for specific and legislative purpose;
- Adequate and relevant to what is required and
- Keep accurate store in a form that permits identification of data subjects;
- Maintain security and confidentiality of personal data.

Author's tips on how to safeguard your privacy online

In India, the digital signatures are issued by certifying authorities who are supervised by the Controller of Certifying Authorities. Digital signatures offer encryption facility using PKI (Public Key Instructor) that uses asymmetric cryptography to secure any email message which are digitally signed. Use of electronic signatures ensures that the content remains untampered and reaches the intended recipient only. In India, TCS is one such organization issuing digital signatures.

- **Read terms of use and privacy policy**- Before using any services on Internet, it is important to read the terms and conditions and privacy policy of that service, to know what personal information is being sought, how data collected will be used or disclosed and in whom the copyright in pictures or content posted by a user will vest.
- **Use electronic signatures & encryption**- It is advisable to use electronic signatures to safe guard your electronic communications. A popular app, WhatsApp uses end to end encryption to protect personal data of its users.
- **Subscribe to DNC Registry**-In order to block telemarketing calls, it is important to use 'do not call registry' service available in India. The Telecom Regulatory Authority of India (TRAI) has framed Telecom Unsolicited Commercial Communications Regulations,2007 for controlling the unsolicited marketing calls telecom, operators to maintain a private 'do not call list'.
- **Change passwords**- It is advisable to keep changing frequently your password of electronic accounts and include both upper case and lower case letters and numbers within it.
- **Two step authentication**- It is advisable to use two steps authentication process using OTP and SMS alert, picture password are common methods for authentication.
- **Beware of vishing/smishing attacks**- Cybercriminals often call or message gullible people by impersonating a bank officer or other service provider and ask for personal information on pretext of conducting verification. One should never share any personal information in case we receive such calls or messages.
- **Careful use of plastic money**- Plastic money should be used with caution and untrustworthy websites should not be used for making electronic payments. It is advisable to pay on a website only when it contains a https protocol, using SSL (secure Socket layers). Plastic money should be used with caution and not allowed to go out of sight since there is growing misuse due to cloning machines.

- **Use an 'anti spyware'** – One should use an anti-spyware before downloading any software or any file such as an email attachment to check for key logger or other kinds of malware.
- **Beware of hidden webcams**- It is important to be vigilant while using any service such as ATM or other areas such as changing rooms in malls.
- **Don't click personal objectionable images**- It is important to educate all not to click personal objectionable selfies/photos or upload or post them on internet.
- **Use incognito mode**- In order to conceal one's identity websites such as LinkedIn offer privacy viewing mechanisms. Also, most browsers allow one to surf the web using incognito window. There are several tools available, some of which are free that allow one to surf the net anonymously and keep your data safe.

  (i) ***Tor Browser***: The Tor Network which is also known as the Onion Router enables anonymous browsing;

  (ii) ***Cyber Ghost BPN***: Cyber Ghost VPN is a virtually privacy network application that reroutes Internet Traffic to conceal one's location and identity;

  (iii) ***Ghostery***: This privacy tool safeguards you from being tracked through behavioral advertising;

  (iv) ***Key Scrambler***: This is a small application which encrypts every letter we typed in a web browser and protects one from key loggers.

  (v) ***Anti-spy for windows 10***: disables advertising IDs, Smart Screen Filtering;

  (vi) ***GNUPG***: It is a short form for GNU Privacy Guard. It is the open source version of PGP (Pretty Good Privacy), Tools for encrypting files;

  (vii) ***Tails***: The free privacy software is based on GNU/LINUX comprising of a browser, monitoring, email and office applications to protect one's privacy;

  (viii) ***Wise folder Hider***: It is designed for window XP, and is a free privacy software which hides things which are put on your computer.

Conclusion

Like our safety, our privacy is in our hands! Prevention is better than cure and this e-book is an easy book that aims to share how to safeguard one's privacy online. The author hopes that readers will benefit from this information. Incase you have any queries, feel free to write to me at karnika@sethassociates.com. While we are making consistent efforts to strengthen our legal framework to protect our privacy and develop new technical tools to preserve and protect our privacy, there are always new challenges emerging in cyber space affecting our privacy. One of the key emerging concepts is the cloud computing. Important considerations concerning privacy will have to be examined in this regard. Cloud computing involves parties from multi jurisdictions. In cloud computing more than one service providers may be used to collect and process data which may involve complex issues of privacy, Data Chain Authentication, Security Procedure to check source and tampering and determination rights and obligations of parties, disclosure reforms and Data Retention Rules. Another emerging concept is the growing use of blockchain technology wherein list of records termed blocks is secured using cryptography.

Each block contains a hash pointer as a link to previous block, time stamp, and a transaction data. The technology lends authenticity to a transaction as the record cannot be altered retroactively without alteration of all subsequent blocks. It brings forth interesting questions about privacy as transactions of individuals and their identity can be easily traced. This technology is also used in bitcoins used in Darkweb activities. Our laws will need to align itself with these emerging concepts in cyberspace. Much awaited is the verdict in Aadhar case which will also throw light on whether collection of sensitive data by Aadhar is or not violative of one's right to privacy (and also whether homosexuality should be criminalized? A linked question is also whether Aadhar has technology robust enough to protect the sensitive biometrical data of Indian citizens it collects? Moreover whether or not it lead to more cybercrimes, such as identity theft or cheating by personation or frauds? Another interesting question to be determined is whether DNA Profiling bill will be passed and made an enactment soon? The first DNA Profiling Bill was prepared in 2007 and has been revised many times. The latest is the "Use and Regulation of DNA Based Technology Bill, 2017." Now that the Right of Privacy has been upheld as a Fundamental right, its provisions will need a tighter scrutiny in terms of safeguards to maintain its security, and ensuing consequences for any violations!