Privacy and Freedom Issues in Cyberspace with Reference to Cyber Law

Indu Sharma
Jamia Hamdard University
Faculty of Engineering & Technology
New Delhi-62, India

M. Afshar Alam
Jamia Hamdard University
Faculty of Engineering & Technology
New Delhi-62, India

ABSTRACT
Privacy and freedom issues in cyber security with reference to IT law takes on important new meaning in cyberspace. Privacy and freedom of expression is said to be universally known for any individual's fundamental right. But when we talk about these right in terms of cyber space, meaning comes out to be very different. Our constitution have various laws regarding this, how these laws plays different role when evaluated online and offline privacy and freedom of expression. This comes to be true when the source of the information is outside the jurisdiction of those endeavoring to control speech. Cyber world is both informational and interactive with lots of autonomy. As everything is available on internet which people do for their personal convenience including personal details, professional details, bank details, and even private keys of individuals. All these information can lead to a serious privacy risk. Along with that how much private data of an individual should be accessible to government. Also, Hate speech on internet, or speech designed to target, oppress or incite hatred or violence against a person or group based on cast, creed, race, religion, nationality, gender, sexual orientation, disability or other group characteristic, do not get effected by locations, time and boundaries. Due to the freely available internet services worldwide, incidents of profane talk has become known throughout the world within seconds and can cause serious repercussion. India presently does not have any specific legislation governing data protection or privacy especially in IT law. However, as per Article-21 which gives right to privacy and Section- 19A which deals with freedom of expression under The Constitution of Indian but still there working is not actively involved when it comes under cybercrime. Although India has come up with IT Act, 2000 and the subsequent amendment to it in 2008 yet it is not able to cover the complete boundaries of cybercrimes, like a very crucial issue of right to privacy. This only shows the imbalance between age old procedure adopted in India and the advancement which Indian society has made. The session focuses on the dynamics of cyber world with respect of privacy concerns and freedom issues with special reference to cyber laws of countries like India, European Nations and United States of America. The problem of how to reconcile all the conflicting claims arising out of the issues of privacy in the context of Internet exposure and the right to freedom of speech. The paper will raise all these issues and discuss the legal implications on the intrusion of the freedom of speech along with some case studies on privacy intrusion.

Keywords
Cyber, cyberspace, freedom of speech, privacy, cybercrime.

1. INTRODUCTION
The endless growth of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called 'Cyberspace'. This cyberspace has become a platform for a galaxy of human activities which converge on the internet. In fact, it promotes all sort of activities which are prohibited by law. The Constitution of India does not patently grant the fundamental right to privacy. However, a legal framework for the cyber world was adopted by India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000 which was amended in the year 2008. The Information Technology Act, 2000 (also known as IT Act-2000) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. This law deals with the cybercrime and electronic commerce. This Act deals with many issues but when it comes specifically to Internet privacy and freedom of expression in cyberspace, the act lacks somewhere because in India this two issues comes directly under constitution of India under Article-21 (right to life and personal liberty) and Article 19A (freedom of speech and expression) respectively. There have been many cases in which it is difficult to differentiate between privacy under civil law and internet privacy with encroachment of freedom of expression. It's high time to introduce these fundamental issues in IT Act, 2000. Though the government has mandated checks for monitoring and protection of user privacy-- it is largely absent. In effect, all Internet traffic of any user is open to interception at the international gateway of the bigger ISP from whom the smaller ISPs buy bandwidth. Since cybercrime is not a matter of concern for India only but it is a global concern and therefore the world at large has to come forward to stricture upon this hazard. When we look up to U.S. Federal Cyber Crime laws and compare it to the India's IT Act, we see a lot of difference when dealing with privacy and freedom issues. Internet privacy should be a legal right to any individual or institution, if the privacy is violated by any mean then user has full right to seek legal actions against it as it is considered as the cybercrime. However, to deal with this type of internet crime, a law has to be enforced specially in IT Act 2000. There have been made many amendments in IT Act but nothing focuses on internet privacy and freedom of expression. Internet privacy should include the user's right to control the information, the user should have all the right to decide whether to allow others to collect, access or use his information and the right to access judicial relief which gives the user right to bring a civil suit against any institution or individual engaged in infringement on his privacy.

1.1 Cyber Crimes in India

Cybercrime is a rapidly growing area of crime. Many criminals use the rapid, real time nature of computer to conduct many criminal activities which could result in serious harms and many dangerous outcomes. New trends of cybercrime evolved every time with the increase of new technology. So, where these new technology is helping people to make life easy and efficient, it is also true that these emerging technology giving chance to criminals to conduct activities which can harm a person, organization, a community or even the whole country. As per the global economy crime survey, there is net loss of thousands of dollar a country has to bear each year. It is noted that United States of America has reported maximum number of crimes among all the countries which is 23%, and when this is compared with India it is only 3%, but, India is a developing country hence with growing technology and user awareness more crimes are taking place. After only some fraction of time, India also will have high percentage of cybercrime if no strict measures are implemented on time. In a study[18], India has found number of cases registered under IT Act are more than that of IPC. So, it is pretty evident that with the growth of technology, crime rate is also rapidly increasing day by day. To control these cases, India has to work upon more strict laws and regulations. Most of these cases belong to privacy violation and freedom of individual. Government has to take strict step to counterfeit these crimes and need to work upon on defining a clear definition of privacy violation online and offline. Following table indicates the study of all India number of cases being registered under IT Act and under IPC.

	IT Act		IPC	
Year	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
Total	9023	4804	2360	2198

Cybercrimes could be in any form from user privacy violation to hate speeches or any other crimes in which a computer or electronic device and a network has been involved. These crimes knows no boundaries, time and location. Even they can be conducted by anyone irrespective of any gender or age group. These crimes not only effect an individual but also the whole community. Today, blogs, Twitter, Facebook, Instagram, community websites and other web-based platforms allow users to reach out to millions of people at the click of a mouse. Generally criminals look for the area or network which is very much prune to attack. And, after these findings, attacker make a strategy to attack in these areas. Some of the crimes listed above are described below:

- **Trademark Violation:** It is the criminal activity in which a criminal use unauthorized trademarks which looks similar or identical to authentic trademark without any licenece.to sale his unauthentic products. This gives confusion to people about the product authenticity. Trademark violation is a kind of "infringement" and the person who performs this is known as "infringer". For example, a fraud website can display a genuine product online and when it gets delivered to concerned buyer it is generally comes out to be duplicate with a label which looks very much similar to actual brand. In the United States, the Trademark Counterfeiting Act of 1984 criminalized the intentional trade in counterfeit goods and services.
- **Religious Offence:** Religious offense means any action which offends religious sentiments and arouses serious negative emotions in people with strong belief and which is usually associated with an orthodox response to, or correction of, sin. India is a diverse country with many religion, and some religious groups try to prove their religion supreme then others. These brings lots of clashes between various communities and could lead to dangerous outcomes. This type of crime is considered as hate crime, and these leads to offline consequences of online religious expression. Serious type of consequences could take place like killing of Blogger or account holder etc.
- **Violence:** Violence is a term which is generally used offline in terms of physical violence, but what about mental violence which is a result of freedom of expression over net. For example, stalking, it is an activity by the means of computer device and network to harass an individual, a group or an organization. There could be any type of stalking, stalking by stranger, Gender-based stalking, of close partners, of celebrities and public figures, corporate stalking.
- **Nigerian scams:** This scam went viral in the recent history. This scam is basically involves offering you large sum of money on the condition you help them to transfer it out of their country. Also, in some cases, they want your contact details along with your bank account details so that they can use this information in money laundering. For example, scammer will tell you a fake story about how his large amount of money is stuck somewhere and he is not able to access it, for this to happen he will seek your help. These scams are commonly known as 'Nigerian 419' scams because the first wave of them came from Nigeria. The '419' part of the name comes from the section of Nigeria's Criminal Code which outlaws the practice. This scan has become so common nowadays that it can come from anywhere in the world.
- **Copyright infringement:** It is a crime in which a user takes up hold on your work without your incant or knowing. Generally owner does the patent of his work which indicates no one can use his work in future because all the rights are with the author only. There is a copyright law in India which clearly protect "intellectual property" rights of an individual.
- **Defamation:** Internet is cheap medium to spread rumor about an individual. Defamation is an act to hurt someone's sentiments by writing or speaking.

If these words are written by the means of computer then it is considered to be cyber defamation crime. It could lead to civil as well as criminal proceedings against the defamer. In common terms it is considered as cyber bullying, which is very much common in young teenagers. This bullying not only hurt the sentiments of a person can also brake down the person morally and emotionally.

- **Government criticism:** India is a democratic country in which all the political parties are elected by its citizens. But computer has become a core source in criticizing government. Criticism is good as India is a free country but using the power of freedom of expression could lead to serious terror among people in which they are compelled to think about the government work, and sometimes these critics are so fake, that people start to think as if it is all true. This image is a result of bias attitude of people who are involved in doing this.
- **Hate speech:** Hate speech is the speech that attacks a person or group on the basis of attributes such as gender, ethnic origin, religion, race, disability, social class, occupation, ideology, appearance, mental capability or sexual orientation. This hate speech are conducted in the form of videos and then they are being uploaded on internet and lots of viewer watch them. Hate speech and freedom of expression need to make a balance between social wellbeing and individual personal liberty. Hate speech has become a fashion nowadays to attract publicity.
- **Impersonation:** Impersonation is an act of pretending to be another person by stealing his identity for the purpose of fraud or entertainment. It is similar to the identity theft. Identity theft typically involves stealing very specific personal information, like a social security number or a credit card number. It often involves much more than using the name or telephone number of another which generally happens in Impersonation. They are both serious king of crimes which not only can result to financial loss but also mental loss or dignity loss.
- **Seditious activity:** activity of showing up dissatisfaction, resistance, or rebellion attitude against the government in power. This can be conducted by words or speeches which can excite people to take steps against the government. These are the activities which are anti-national in nature. This is a very serious crime and it is defined by Section 124A of the Indian Penal code. These activities can turn up into very harsh as it can lead to serious dispute between public and government.
- **Privacy and security:** There are almost 21% of the crimes related to privacy and security. In Indian law, privacy has no clear definition as online privacy and offline privacy clause. All these crimes are treated under the same umbrella. Sensitive personal information when get leaked there is huge risk of security so privacy and security goes hand in hand. These risks are different for different sectors. As per a survey 81% of respondent believes that privacy is the biggest risk when talk about cybercrimes.

1.2 Laws related to privacy and freedom of Expression

1.2.1 Law in India[27]

India is the host and the biggest platform of data outsourcing. It needs an effective and well formulated way of dealing with these crimes. Unlike many other countries like EU, India does not have any separate law which exclusively deals with the data protection. However, the courts on many cases have interpreted "data protection" within the limits of "Right to Privacy" as implicit in Article 19 and 21 of the Constitution of India. Apart from this, the laws which are presently dealing with the subject of data protection are "The Indian Contracts Act" and "The Information Technology Act". Some of the Indian laws are listed below:

Article 19 of the Indian constitution states that: All citizens shall have the right —

1. to freedom of speech and expression;
2. to assemble peaceably and without arms;
3. to form associations or unions;
4. to move freely throughout the territory of India;
5. to reside and settle in any part of the territory of India; and
6. to practice any profession, or to carry on any occupation, trade or business

Freedom of speech is restricted by the National Security Act of 1980 and in the past, by the Prevention of Terrorism Ordinance (POTO) of 2001, the Terrorist and Disruptive Activities (Prevention) Act (TADA) from 1985 to 1995, and similar measures. Freedom of speech is also restricted by Section 124A of the Indian Penal Code, 1860 which deals with sedition and makes any speech or expression which brings contempt towards government punishable by imprisonment extending from three years to life.

Section 43A- ITAA The IT (Amendment) Act, 2008 (ITAA 2008) explicitly provides that "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected".

Section 72A. Punishment for Disclosure of information in breach of lawful contract that "Punishment for disclosure of information in breach of lawful contract. -Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both".

Both the above sections don't deal with data privacy and security directly. Before 2011, the situation of privacy laws was very much confusing, ambiguous and vague because

there was no law which could directly deal with this issue. But after 2011, when EU has applies very strict and stringent laws related to data protection, the Indian government also felt the need of making certain changes in our country.

Section 69A can deny public access to any information through any device. By this rule, Government can interfere with the privacy of data in certain conditions to maintain the integrity of India, defense 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 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. This rule gives the power to Government to interfere, monitor or decrypt any data including information that is personal in nature of any computer device.

1.2.2 Laws outside India, with focus on EU and US laws

EU legislative[36]

Article 16 protects the confidentiality of personal data, by prohibiting any person who has access to personal data to process them "except on instructions from the controller, unless he is required to do so by law.[37]

Article 17 of Directive 95/46/EC mandates the undertaking of "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."[37]

The European Commission has played a key role in the development of European cybercrime center as termed as EC3, which started operations in January 2013. EC3 acts as the focal point in the fight against cybercrime in the Union, pooling European cybercrime expertise to support Member States' cybercrime investigations and providing a collective voice of European cybercrime investigators across law enforcement and the judiciary.

Data protection is a fundamental right enshrined in Article 8 of the EU Charter of Fundamental Rights, which is distinct from respect for private and family life contained in Article 7 of the Charter.

Article 19(3) Freedom of expression. A number of potential restrictions on the right to freedom of expression are contemplated by European laws, including laws on telecommunications; racial hatred; copyright; privacy, and censorship in classification and broadcasting. A number of these laws are based on valid grounds for restriction referred to in article 19(3) of the ICCPR. However, questions remain as to whether some of these laws would meet the levels of transparency and proportionality required by article 19(3).

US laws[38]

Privacy Act (1974)

There appear to be 3 types of "privacy" interests protected by Constitution:

- Freedom from govt. surveillance and intrusion (4th Amendment)
- Avoiding disclosure of personal matters (14th Amendment)
- Independence in making important personal decisions (primarily 14th and 9th Amendments)

The 1st Amendment Freedom of speech in cyberspace.

1.3 Current Trends of privacy in digital forensics

Currently privacy of an individual or organization has been intact with the help of a form filling specially if a person is making an account online or if he is joining a group or company. Certain kind of identification is required for authenticity. When authenticity of the person id done, then other security principle like confidentiality and integrity are work upon.

Following are the rules while creating an account online:

- Person has to add his basic details like name, country, city, address, phone number, email address etc.
- If the account is bank account or any other account in which money is involved then a password is created every time when login
- This password is sent to the person's phone number as OTP, by using which user can access to his account and do the processing.
- This OTP assures that user is authentic.

The main factor of privacy risk is to decide who is going to violate privacy. Sometimes, these are not only attackers from outside but also the authentic attacker from inside. When user enters or saves his private details online he is assured that his details will remain confidential and organization will not take advantage of his details. For this to happen there is always a confidentiality clause with almost every website, which is kept under supervision with a third party which is generally a government body. But anyhow, if these privacy risks are violated then there are various laws which protect people from unreasonable seizure and searches, and warrants that allow such seizure has to be specific to its cause. However, the laws only restricts what type of information to be searched and seized, not the protocols on how they are to be searched and seized. Government has proposed a structure in which enterprises can meet forensics protocols to detect privacy related violations. It consists of a series of business processes and forensics investigations, and can be executed in a hierarchical manner such that these enterprises can perform quality privacy related forensics investigations protocols on information privacy incidents. There are two other models to investigate privacy breaches. Firstly, a cryptographic model which need to be included into the current digital investigation framework, where forensics investigators first have to allow the data owner to encrypt his digital data with a key and perform indexing of the image of the data storage. They will then extract data from respective image sectors that matches keywords with the encryption key. Image sectors which do not match with the keywords will not be revealed to forensics investigators, which guarantees privacy. Another model is a layering system on data through which user's privacy is maintained and forensic investigators themselves cannot infringe privacy. In this, forensics investigators first obtain information that is layered in the very first layer before moving towards the next layer. As each layer of information is matched and obtained information of the layer gets deeper

and closer in relation to the relevant information until the final layer where actual information lies for forensics investigation and directly linked to the person.

There is one more approach which is used by enterprises, this is Privacy Enhancing Technologies (PET), and this is used to preserve user anonymity while accessing the internet. This technology allows users to continue being anonymous until the server has enough evidence to prove that the user is attacking the network or server. This technology is designed to balance between user privacy and digital forensics.

1.4 Freedom of Expression in India

As we always say that privacy is fundamental right of an individual, there is one more right which should be rewarded as Fundamental right or first condition of personal liberty in a democratic country like India. It occupies a most deserving and important position in the liberty hierarchy. Freedom of Speech and expression means the right to express our own opinions freely by means of words from mouth, writing, typing, printing, pictures or any other mode. In today's time it is accepted worldwide that the right to freedom of speech is the essence of free society and it must be protected all the time. The first principle of a free society is non hampered flow of words in a blog, paper, or in an open forum. Freedom to express opinions and ideas without halt, and especially without fear of getting punished plays significant role in the development of free and open society. It is one of the most important fundamental liberties guaranteed against state suppression or regulation. Freedom of speech is guaranteed not only by the constitution or statutes of various states but also by various international conventions like Universal Declaration of Human Rights, European convention on Human Rights and fundamental freedoms, International Covenant on Civil and Political Rights etc. These declarations openly talks about protection of freedom of speech and expression. When we talk about India, freedom of speech leads a special position. The importance of it can be easily understand by the fact that India is a diverse country with many religions, states, languages etc., but our constitution ensures to all citizens get the liberty of thought, expression, belief, faith and worship. The constitutional significance of the freedom of speech has written in Indian Constitution as fundamental and human right in Article 19(1) (a) as "freedom of speech and expression".

When we talk about cyberspace, how much liberty should be granted on freedom to express, is still an open debate. It is very important that liberty of one must not offend the liberty of others as it should be a moral duty of a person to maintain the dignity of others.

2. LITERATURE REVIEW:

There have been many articles and books published which deals with the privacy issues in internet and freedom of expression. Some of the key points extracted from these articles and journals are consider in this study. An analysis has been made by Chun Cheng Niu which focus on the perception layer of Things layers of security issues and the security policy. Analysis of the privacy issues involved in the Internet of Things applications to the response options. [1] Privacy has given a different meaning by Rehan Khan which discusses on growing privacy issues in cyber space and a legal approach to defend and protect one's privacy rights in India, he focuses more into privacy concerns which have been raised by use of smartphones enabled internet. [2] Ms. Asou Aminnezhad has identified various issues in cyber security and digital forensics, issues that use for protecting privacy of data in forensic investigation, whereby how forensics investigators may have infringed user privacy while conducting forensics investigations, and how user privacy is always under threat without proper protection. [3] Alok Mishra discusses on privacy specially in e-commerce sector, lights into privacy enhancing techniques specially scenario of the platform for privacy preferences(P3P), in his study SSL is used for privacy preserving but more technological advancement is required. [4] Mr. A. A. Sattikar focuses on security and privacy issues in social networking sites, focuses mainly on the possible attacks which can interfere in one's privacy. He also suggested various methods by which one's security and privacy can be enhanced. [5] R. Aggarwal analyzes the cyber laws in India and raises the issues of criticality of provisions relating to dispute resolution in India with special reference to internet access and usage, freedom of expression and privacy issues. [6] Dr V.Kiran Kumar discusses about the privacy and interoperability issues relating to Social Web, he also introduces the semantic web. [7] Tuija Kuusisto explains various emergent phenomena of the cyber world including more critical issues like security planning and privacy control. [8] As per the research of Mahantesh B Madiwalar, he gives more emphasis on data protection and privacy rights with more consideration of e-commerce. He also suggested to bring strong data protection laws in our constitution. [9] Sanaz Taheri Boshrooyeh talks about the security problems in online social networks, there are some functionality to access social networks and these functionality needs to be served in a very secured manner, she has suggested many solutions to counterfeit these security challenges. [10] Albert I. Aldesco talks about Anonymous Speech, Freedom of Association and Inviolable Privacy. Also, in his findings he emphases more on restricting unnecessary outage of access in cyberworld.[11] Ann Beeson states that cyberspace is "probably the richest source of creative, diverse, empowering and democratizing communication ever to connect people across the globe".[12] An International Survey of privacy laws and practices has been conducted which emphasizes more on data protection and associated rights of a person, in which he has full right to willingly decide how much information is required for accessing a webpage[13] Indian cyber law has been explained in [14] [15] in which all sections and articles are explained. Online social networking and their associated risks especially in privacy and security, along with freedom of speech on them has been explained in [16][17][18][19][20][21][22][23][24][25][26]. P. Jain lights upon the risks of sharing mobile number or contact details on social networking sites [28]. Chung, W. & Paynter, J. detail about privacy issues on the internet and in there finding they focuses more into country Huwaii [30]. An annual report on freedom on net has been retrieved by the Freedom House, in which number of different countries have been evaluated and scores are given on the basis of rights of freedom of opinion on the net.[33] European laws of data protection and privacy along with freedom of speech has been given in [36][37]. US Federal computer crimes and related laws copyrighted by SANS institute given in [38]

3. PROPOSED WORK AND IMPLEMENTATION

3.1 Concerns on Privacy

Article-19A of Indian Constitution does not clearly define the crimes related to online privacy and offline privacy. So there are various concerns regarding to the privacy. Some of the biggest concerns are described below:

- **Lack of public interest in gaining knowledge:** people working on internet does not clearly know about how they can protect their data. They even don't know that the websites they visit could be tracked down secretly. When user enters his details then so much information like e-mail addresses and other personal information could be collected and used for marketing, laundering or other purposes without approval of user. These personal information could be sold to a third party for money without the consent of user. To avoid all this user need to aware but most of the user don't want to gain knowledge regarding this.
- **Lack of procedural safeguards against surveillance activities:** some of the activities of user are under surveillance with user consent but there are lack of procedural safeguards which can lead to data leakage. So it is important to ensure that there should be proper safeguards in the form of available software in market to protect the data. When surveillance activity is happening then confidential data should not be kept in open.
- **Scanning in the name of cyber security:** sometimes user data is scanned just to show that it is mandatory for security but when this scanning takes place then it could lead to serious privacy risks. This scanning generally conducted by some non-official resource. Scanned data may contain confidential information about the user.
- **Invisibility to user:** user generally don't have any idea that there personal information has been violated by the means of cookie proliferation in which cookies or sessions of user websites are hacked, seizing cloud data, location data betrayal.
- **Lack of clear definition in IT Law:** Indian IT Law does not have a clear and separate legislative for privacy issues. The crimes related to privacy online are treated in the same manner as that of offline crimes. However, there should be complete unique section of crime based on privacy.

3.2 Right to be forgotten - Privacy in the 21st Century

Right to be forgotten is a next generation "Human Right" as can be envisaged under the United Nations Convention on Human Rights (UNHCR) and is the logical corollary and evolution of the "Right to Life and Personal liberty" considered to be a fundamental Global Human Right. Right to be forgotten is essential for the free and most complete development of our Self, to achieve our utmost potential we need to limit the "infinite memory "(both in space and time) accorded to us by the exponential progress made by science over the course of the last century. Computers, especially the all-pervasive inter connected computing systems processing big data such as those of Google, MS, Apple etc., provide an instant access to the "private sphere" of an individual, where the veil over privacy is almost non-existent. An individual's right to life and personal liberty as guaranteed by UNHCR as well as even the Indian Constitution vide Article 21 will be violated if all past events related to the individual are made available to anyone at the click of a button without any judicial overview. An individual should be accorded the right to "MAKE" an online search provider/aggregator to remove any links pertaining to him/her to ensure their fundamental rights are guaranteed. Many argue that "right to be forgotten" is antithetical to the right to free speech as guaranteed by the Constitution of all democratic countries without realizing that right to free speech is not absolute and doesn't include the right to defame, slander, and invade the private space of an individual; all of which are considered criminal offences. According to a press release "Majority of Americans think it should be able to delete to remove personal information online".[10] but how to grant this access to individual is still a question.

3.3 Freedom of expression-Social wellbeing or personal liberty?

To make a society work efficiently it is important that a person understands his responsibilities towards society and does not do anything that could bring serious hazard to someone else's feelings. Like privacy, freedom of expression also does not have a clear definition in our constitution. So, question is, how much liberty is necessary when we talk about the feeling expressed in digital media in form of social networking sites, blogs and forum. Sometimes this personal liberty can effect other's feelings and sentiments like writing fake story about someone to defame them, writing offensive words to some specific community which can lead to rites. Presently there is no restriction mentioned on the freedom of speech. The government should specifically work upon in the area of deciding how much liberty should be granted to an individual so that it cannot affect others somehow. However there are cases in which it is very much important to protect freedom of speech. Some of the reasons are for the finding of truth by open discussion, free speech is important for self-fulfillment and development, restriction on speech or opinion can hamper personality and growth of an individual. Free speech is important for the welfare of society and one of the key characteristics of democratic society. Thus it is important to protect freedom of speech but there are also some concerns related to the freedom of speech which needs to addresses for an efficient society. These issues are as follow:

- Offensive speech
- controversial ideas
- written words in social networking sites, blogs or forums
- Pictures, videos, art and other forms of expression and opinion
- False speech
- Commercial speech (eg., advertisement)

4 RECOMMENDATIONS

4.1 Technological

This is general assumption that with the technological advancement, solution of privacy protection can be answered. Some software companies have already developed tools and standards that can handle privacy issues.

So, to maintain privacy one should work on the following:

i. Users should be encouraged to use "openvpn" based VPN services by default for all communication

ii. ISPs should offer shared IP connections which offer plausible deniability as long as ISP doesn't log traffic at internal / MAC ID level;

iii. ISPs can offer shared IP VPN / tunneled connections which are in accordance with the law as well as offer plausible deniability - such connections don't need to be "logged" as per India, US and EU regulations - even if logs kept impossible to correlate traffic with source / origin unless other factors used to establish / tie in such traffic. All devices capable of hardware encryption MUST be enabled by default with at least AES 256 or higher - encryption should be opt-out rather than opt-in.Users must avoid key rings wherever possible. In case a user feels comfortable keys must be stored physically separate from the computer / encrypted device (example - keys on a pen drive instead of a password).

iv. Keys may be hidden inside a common / innocuous looking file - steganography hidden in plain sight - this reduces pain of handling physical keys yet increases security multiple folds.

v. Biometric should be avoided as far as possible in place of keys - it offers convenience but is useless for protection (ex - aadhar has our biometrics, fingerprints can be lifted off someone's used glass / razor / bottle etc, facial logins can be faked using high res videos).

vi. Biometrics doesn't offer protection from self-incrimination (art. 20(3) India , 5th amendment US) [application of one's mind against self is protected => you can't be forced to tell your password / give keys but you can be forced to put your thumb / eye on a scanner]

vii. ISPs should be held accountable if default security of CPE provided by ISP is compromised without active customer involvement

viii. Use of Platform for Privacy Preference (P3P) which helps users make informed decisions about when to release their data. Consumers are not waiting for the government or self-regulation. For example, Indian parliament wanted users to retain plaintext copy of all digital communication / files for 60 days - cancelled after uproar in society.

4.2 Combination Solution

It is believed that using a combination solution for privacy and freedom issues can make it possible to protect data and amicably handling of issues raised from freedom of expression. The combination results of legislation, self-regulation, morality and technological solutions may provide an effective solution than a single solution. For example, Civil Society should be encouraged to run Tor/Free-net exit nodes to ensure freedom of communication / dissent (How to balance against national security - price to pay for true democracy?) user should be assured that data and information given to him is used as it has been promised. In this case, legislation and self-regulatory authorities can help to provide such assurances. But somehow, these self-regulation and privacy enhancing technologies are not enough to protect privacy so they need to be accompanied by legislation.

5 CONCLUSION

India need to work more for enduring an effective and concrete legislation for data protection. This new legislation should deal with the protection of data and information present on the cyber world. However, while creating the laws, the legislature has to be well aware for maintaining a balance between the interests of the common people along with amicably handling the increasing rate of cybercrimes. For privacy intactness, proper training and awareness, monitoring and auditing, and incident response is required Expression through speech is one of the basic need provided by civil society. Variance in the scope of freedom of expression, combined with more online communication, has produced concerns about censorship in cyberspace. Freedom of opinion and expression should be free from any kind of political, commercial or any other influences. It should be applied in non-discriminatory and non-arbitrary manner, also, should be supported by applying safeguards against any kind of abuse, hate speeches, religion biasing etc.

6 REFERENCES

[1] Chun Cheng Niu , Kuan Cheng Zou , Yuan Ling Ou Yang, Guan Jie Tang, Yi Zou "*Security and Privacy Issues of the Internet of Things",* September 2013

[2] Rehan Khan "*Cyber Privacy Issues in India*", Article in Social Science Research Network(SSRN) Electronic journal, DOI: 10.2139/ssrn.2357266, January 2013

[3] Asou Aminnezhad, Ali Dehghantanha, Mohd Taufik Abdullah *"A Survey on Privacy Issues in Digital Forensics",* International Journal of cyber security and digital forensics, The society of Digital Information and wireless communication, 2012(ISSN: 2305-0012)

[4] Alok Mishra, Deepti Mishra, *"Web Privacy ; Issues, Legislations and Technological Challenges",* DOI: 10.4018/978-1-59904-804-8.ch001 **,** September 2008

[5] A. A. Sattikar , Dr. R. V. Kulkarni "*A Review of Security and Privacy Issues in Social Networking"*, International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2784-2787.

[6] R. Aggarwal "*Dispute settlement for cyber crimes in India: An analysis*", DOI: 10.4018/978-1-4666-4209-6.ch015, January 2013

[7] Dr V.Kiran Kumar, "*SEMANTIC WEB APPROACH TOWARDS INTEROPERABILITY AND PRIVACY ISSUES IN SOCIAL NETWORKS*", International Journal on Web Service Computing (IJWSC), Vol.5, No.3, September 2014.

[8] Tuija Kuusisto, Rauno Kuusisto, "*Cyber World as a Social System"*, DOI: 10.1007/978-3-319-18302-2_2 , January 2015
In book: Cyber Security: Analytics, Technology and Automation, Publisher: Springer, Editors: Martti Lehto, Pekka Neittaanmäki, pp.31-43

[9] Mahantesh B Madiwalar, Prof(Dr.) B S Reddy "Privacy Rights and Data Protection In Cyber Space with Special Reference to E-Commerce", Global Journal for Research Analysis, Volume-4, Issue-12, Dec-2015 • ISSN No 2277 – 8160.

[10] Sanaz Taheri Boshrooyeh, Alptekin Kupcu, Oznur Ozkasap "Security and Privacy ofDistributed Online Social Networks", Conference: IEEE ICDCS (International Conference on Distributed Computing Systems) Workshop ESP-DGC, At Columbus, Ohio

[11] Albert I. Aldesco, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, 23 Loy. L.A. Ent . L. Rev. 81 (2002).

[12] Ann Beeson, Top Ten Threats to Civil Liberties in Cyberspace, HUM.RTS., Spring 1996, at 10, 10

[13] Privacy and Human Rights, An International Survey of Privacy Laws and Practise, Global Internet Liberty Campaign at www.gilc.org/ privacy/survey/intro.htmlaccessedon23rd August,2013

[14] Gupta, Rohit K. (2013). India : An Overview of Cyber Laws vs. Cyber Crimes : In Indian Perspective at www.mondaq.com accessed on 4th December,2013

[15] Report on 'Cyber Security and Right to Privacy' submitted by the Parliamentary Standing Committee on Information Technology presented on Feb. 12, 2014 under the Chairmanship of Rao Inderjit Singh to the fifteenth Lok Sabha.

[16] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, pp. 29–42, ACM, 2007.

[17] S. R. Chowdhury, A. R. Roy, M. Shaikh, and K. Daudjee, "A taxonomy of decentralized online social networks," Peer-to-Peer Networking and Applications , pp. 1–17, 2014.

[18] https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

[19] M. Beye, A. Jeckmans, Z. Erkin, P. Hartel, R. Lagendijk, and Q. Tang, "Literature overview-privacy in online social networks," Centre for Telematics and Information Technology, University of Twente, 2010.

[20] S. Jahid and N. Borisov, "Enhancing security and privacy in online social networks," Technical Report, Illinois University, 2012.

[21] A. Sattikar and D. R. Kulkarni, "A review of security and privacy issues in social networking,"International Journal of Computer Science and Information Technologies , vol. 2, no. 6, pp. 2784–2787, 2011

[22] E. Novak and Q. Li, "A survey of security and privacy in online social networks," College of William and Mary Computer Science Technical Report , 2012.

[23] M. M. Lucas and N. Borisov, "Flybynight: mitigating the privacy risks of social networking," inProceedings of the 7th ACM workshop on Privacy in the electronic society , pp. 1–8, ACM, 2008.

[24] A. J. Feldman, A. Blankstein, M. J. Freedman, and E. W. Felten, "Social networking with frientegrity: Privacy and integrity with an untrusted provider.," in USENIX Security Symposium, pp. 647–662, 2012

[25] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin,"Persona: an online social network with user-defined privacy," in ACM SIGCOMM Computer Communication Review, vol. 39, pp. 135–146, ACM, 2009

[26] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," Network, IEEE, vol. 24,no. 4, pp. 13–18, 2010

[27] Cyber laws related to privacy and freedom issues retrieved from http://www.cyberlawsindia.net/lawyering.html

[28] P. Jain, P. Jain, and P. Kumaraguru, "Call me maybe: Understanding nature and risks of sharing mobile numbers on online social networks," in Proceedings of the first ACM conference on Online social networks, pp. 101–106, ACM, 2013.

[29] Joshi and C.-C. Kuo, "Security and privacy in online social networks: A survey," inMultimedia and Expo (ICME), 2011 IEEE International Conference on, pp. 1–6, IEEE, 2011

[30] Chung, W. & Paynter, J. (2002). Privacy issues on the Internet. Proceedings of the 35th Hawaii Internaional Conference on System Sciences.

[31] Davis, J. (2000). Protecting privacy in the cyber era. IEEE Technology and Society Magazine, Summer, 10-22.

[32] Earp, J.B., Anton, A.I., Aiman-Smith, L., & Stufflebeam, W.H. (2005). Examining Internet privacy policies within the context of user privacy values, 52(2) 227237.

[33] Article: By freedom house – About freedom on the net. Retrieved from https://freedomhouse.org/report-types/freedom-net

[34] Frank Y.W. Law et al, "Protecting Digital Data Privacy in Computer Forensic Examination," Systematic Approaches to Digital Forensic Engineering (SADFE), 2011.

[35] "Cyber Crimes and the Society", Post Graduate Diploma in Cyber laws & Cyber Forensics, Distance Education Department National Law School of India University, p-84.

[36] European Union Agency for Fundamental Rights retrieved from http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

[37] Maria Grazia Porcedda, "DATA PROTECTION AND THE PREVENTION OF CYBERCRIME: THE EU AS AN AREA OF SECURITY?", EUI Working Papers, European University Institute, Department of law

[38] U.S. Federal of computer crime by SANS Institute is retrieved from https://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446