Page 1388 - 1397

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 3

2020

Privacy Issues in Cyber World

ANISH ROY[1]

ABSTRACT

In the early days when printing press was the only medium available to the journalist he had enough time to study and edit the news which he would perhaps publish in a newspaper or article for the consumption of the general public. But with the advent of the Internet and the information age the onus lies on quick delivery of news which left the journalist with little or no scope for editing. Today most cyber editors agree that the standards should be the same whether publishing online or in print. As cyber news becomes a bigger component of how people in the developing countries like India get news, the practices of cyber news journalists become all the more important. Cyber journalism raised many challenging ethical concerns, including issues in the areas of privacy, advertising, business relationships, copyright, attributions, linking, posting supplementary materials, manipulation of data and graphic images. In this context, Jay Black wrote, "the bottom line (is that) new media technology and delivery systems make it necessary for individuals journalists to develop more sophisticated ethical decision making skills". It is now well known that privacy is a human right since it has been recognised by the United Nations Declaration of Human Rights and many national and international treaties. Almost all the countries recognize privacy as a fundamental right of its citizens. Some countries have this right inherent in their constitution like South Africa and Hungary, while others with old constitutions have recognized it through other provisions. Most of the privacy laws in various countries are set on the guidelines prepared by the Organization for Economic Cooperation and Development and the Council of Europe. Threats to privacy of ordinary citizens in the wake of increased use and up-gradation of information technology have made the task more daunting for lawmakers worldwide.

I. INTRODUCTION

In the early days when printing press was the only medium available to the journalist he had enough time to study and edit the news which he would perhaps publish in a newspaper or article for the consumption of the general public. But with the advent of the Internet and the information age the onus lies on quick delivery of news which left the journalist with little or

[1]Author is a student at KIIT School of Law, Bhubaneswar.

 [ISSN 2581-5369]

no scope for editing. Today most cyber editors agree that the standards should be the same whether publishing online or in print. As cyber news becomes a bigger component of how people in the developing countries like India get news, the practices of cyber news journalists become all the more important. Cyber journalism raised many challenging ethical concerns, including issues in the areas of privacy, advertising, business relationships, copyright, attributions, linking, posting supplementary materials, manipulation of data and graphic images. In this context, Jay Black wrote, "the bottom line (is that) new media technology and delivery systems make it necessary for individuals journalists to develop more sophisticated ethical decision making skills". It is now well known that privacy is a human right since it has been recognised by the United Nations Declaration of Human Rights and many national and international treaties. Almost all the countries recognize privacy as a fundamental right of its citizens. Some countries have this right inherent in their constitution like South Africa and Hungary, while others with old constitutions have recognized it through other provisions. Most of the privacy laws in various countries are set on the guidelines prepared by the Organization for Economic Cooperation and Development and the Council of Europe. Threats to privacy of ordinary citizens in the wake of increased use and upgradation of information technology have made the task more daunting for lawmakers worldwide.

II. TRENDS IN PRIVACY INVASION

Privacy International has identified a number of important trends that contribute to privacy invasion[2].

1. Globalisation which removed geographical limitations to the flow of data, one of the best examples of which is the Internet.
2. Convergence which is leading to the elimination of technological barriers between systems. Modern information systems are interestingly interoperable with other systems and can mutually exchange and process data.
3. Multimedia which fuses many forms of transmission and expression of data and images so that the information gathered in a particular form can be translated into other forms.

III. PRIVACY INVASION IN THE CYBER WORLD

Cyber-crimes or a crime committed in the virtual world of the Internet wherein "the computer is either a tool or target" is the most pervasive of all forms of privacy intrusions in the

[2] Nair, Pradeep (2008). Cyber Journalism Legal and Ethical Issues, Media Law and Ethics : Readings in Communication Regulation, edited by Kiran Prasad, B.R. Publishing Corporation, New Delhi

 [ISSN 2581-5369]

modern world. Owing to the extensive use of the Internet and technological up gradation in the e-world people use the Internet for a wide variety of purposes which include social networking sites such as Facebook, Twitter, LinkedIn. These sites have more than 400 million users and applications such as chatting, uploading, photographs and others have the capacity to retain a lot of private information in their databases[3]. Wikipedia says internet privacy involves 'the right or mandate of personal privacy concerning the storing, repurposing[4], provision to third parties and displaying of information pertaining to oneself in the Internet." Internet users can minimise the risks of privacy intrusions through controlled disclosure of personal information such as revelation of I.P. address and non-personally identifiable profiling. In today's world companies are hired to watch what internet sites people use and collect the information to create a database for marketing purposes. More malicious acts concerning invasion of privacy include spreading of spyware and the exploitation of various forms of bugs (software, faults). Children and adolescents using social networking sites are easy prey for privacy intruders as they can easily track any information fed by them on the Internet. Threats may include e-mail scams and attachments that get them to install malware and disclose personal information. In 1998, the Federal Trade Commission in the US considered the lack of privacy for children on the Internet and created the Children Online Privacy Protection Act (COPPA). In 2000, Children's Internet Protection Act (CIPA) was developed to implement safe Internet policies such as rules and filter software. These laws, awareness campaigns, parental and adult supervision strategies and Internet filters can all help make the Internet safer for children around the world[5].

The protection of privacy is one of the most important issues on the Internet today and is of concern to the users of the Internet. Websites are collecting personal information from users through online registrations, surveys and forms. Information is also collected from users with 'cookies'. Under the European Directive on Data Retention, the destination of a communication, the date, time and duration of a communication, the type of communication, the communication device and the location of mobile communication equipment can be recorded. Under the European Directive[6], it is not necessary for a judicial warrant to be sought before data is made available to investigators. Rob van den Hoven van Genderen (2008)[7] in the discussion paper 'Cybercrime investigation and the protection of personal data

[3] Black, Jay (1994). Aeropagitica in the Information Age, Journal of Mass Media Ethics, 9 (3), 134.
[4] Internet Privacy (2014 June 19)in TheWikipedia: The Free Encyclopaedia. Retrieved 03.43, July 17, 2014, http://en.wikipedia.org/w/index.php
[5] Westin, Alan F. (1967). Privacy and Freedom, Athenum, New York.
[6] Id
[7] Genderen, Rob van den Hoven van (2008),Cybercrime Investigation and the Protection of Personal data and

 [ISSN 2581-5369]

and Privacy' published by the Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, Strasbourg, says that because of the globalization of economic, political and social activities along with increasing use of the Internet, a wide range of issues need to be addressed regarding privacy and protection of personal data. These pertain to preserving the privacy rights of individuals without hampering the free flow of information and the extent to which the authorities are free to use personal data and the sources which can be tapped to extract the data often available in government databases[8]. The other key questions are: how can the tension between privacy protection and criminal investigation be regulated at acceptable levels? And; what adaption's to the existing regulatory framework are needed?

IV. CONTROL OF PRIVACY INTRUSIONS IN THE CYBER WORLD

Cybercrime investigations need to take into account privacy concerns while implementing the procedural provisions of the Convention on Cyber Crime. Cybercrime investigations require more technical expertise and surveillance than conventional crime but it also needs to be ensured that here is protection of fundamental privacy principles both in the national and international law. As basic principles for the protection of privacy there are three international treaties that are widely recognized as the basis for the protection of privacy and personal life: Article 12 of the Universal Declaration of Human Rights of 1948, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).The OECD guidelines on the Protection of Privacy and Trans border Flow of Data are also of relevance in this aspect[9]. Alan Westin (1967) in 'Privacy and Freedom' defined privacy as the 'desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.

However, measures taken to punish and prevent terrorism have tilted the balance towards security protection at the cost of individual privacy. Though international treaties do recognize the preservation of privacy as an important component during the use and processing of personal information however recognition of the right to privacy is no guarantee that it is actually followed in national practices.

Privacy, Report for Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg,France at www.coe.int/cybercrime

[8] Chaudhuri,Prasun,'I'm going to ruin you, DEAR',3rd August,2014,The Telegraph at www.telegraphindia.com accessed on 3rd August,2014

[9] Gupta, Rohit K. (2013). India : An Overview of Cyber Laws vs. Cyber Crimes : In Indian Perspective at www.mondaq.com.

 [ISSN 2581-5369]

It is true that knowingly or unknowingly a lot of information is uploaded by us on the Internet which can be used by a criminal for harassment or for committing a crime. The crime may involve the data provided by the person or the physical person himself. This is called cyber stalking where the stalker uses the Internet or other modes of electronic communication to harass the personas the virtual world of the Internet provides the stalker with anonymity. In this context, the harassment of the victim due to concealing of identity of the stalker assumes significance. The methods of contact adopted by cyber stalkers include Live Chat or IRC (Internet Relay Chat), Message boards and newsgroups, e-mail and data brokers. Data brokers are the people who sell information collected from private databases.7 Due to immense increase of Internet use, incidences of cyber-crime or crimes involving use of computers coupled with the use of the Internet is on the rise globally. The reasons for the same are not difficult to find. Because of the increased dependence of the people on the Internet for information the number of users has raised dramatically a large section of whom are not aware of privacy intruders lurking in their shadowy world[10].

A recent form of crime on the Internet sweeping across the world-from developed countries to developing and poor countries alike is revenge porn. The crime has spread its tentacles into Indian lives also as the use of the Internet and use of social networking sites increases in Indian homes along with the use of smart phones by Internet-savvy kids. The profile of the criminal in revenge porn is usually different from other cyber-crimes and the accused may be a friend, partner, relative or colleague with no criminal history. Mostly the sexually explicit pictures are of ladies posted by revengeful lovers or spurned men who are keen to defame the women. With the increasing use of sophisticated mobile cameras people mostly girls often take photographs while taking a bath or in inner wear and share them with their boyfriends nonchalant of the dangerous consequences of their act. Cyber-crime experts feel that they do it to show off as symbols of independence or defiance. According to reports there are at least 3000 voyeuristic websites where such pictures can be posted. These clips are often copied and replicated across multiple porn sites, making it virtually impossible for the authorities to wipe off the digital prints. Incidences of such crimes where sophisticated technology is used by the criminals is on the rise as people especially teenagers are hooked on to extensive social networking site use.

In our country, though Sec 66 (E) of the Information Technology Act 2000 criminalises the publication and transmission of images of an individual's private parts without consent and Sec 354[C] of the Criminal Law (Amended) Act 2013 criminalises capturing and sharing

[10] The State of Privacy (2014). Privacy International at www.privacy.org

 [ISSN 2581-5369]

images of a woman in private space, yet strong affirmative action from both the executive and judiciary is needed to tackle this menace. In this context, a step in the right direction has been taken by Israel which has declared posting of images without consent as sexual harassment, punishable by up to five years in jail. Similar laws are also in the pipeline in the UK and the US which can be emulated by India for safeguarding the privacy of its citizens.

V. TECHNOLOGY AS A FACILITATOR

In our daily life when we visit a store, see a doctor; visit a bank or a library, data of our actions and transactions will be recorded and stored in databases. This generates digital footprint based on our activity data which is gathered from digital communications and service actions that may include a click of the mouse or RFiD reader record. Because of convenience, we are used to smart cards, debit card, benefit card and others. Intelligent devices such as smart cards facilitate creation of personal profiles that indicate behavioral patterns and picture of our lifestyle. Today we live in a networked world where ubiquitous technologies offer many benefits like smoother and effortless services and also enhance our ability to communicate about ourselves as well as our needs. These technologies enable collection processing and utilization of different types of information which can be easily put under surveillance using refined and up to date tools. The privacy violations perceived under an ubiquitous environment are based on the fact that the user will lose control of the data concerning his activities[11]. We know that Web 2.0 has empowered users to chat freely with friends, speak directly to customers, service representatives, check store online and other innovations which leave a digital trail that can be used to violate the privacy of the user and his security. Even one's reading materials and articles are now in the public domain on sites such as Facebook and Amazon[12]. The concern of data analysis being done to scan the intimate details of citizens across the world has now extended to humanitarian organizations and the United Nations. The UN High Level Panel on the post 2015 Development Agenda has called for a 'New Data Revolution' and the movement is being spearheaded by the United Nations Global Pulse and UNICEF Innovation. The World Bank, World Economic Forum and the Organization for Economic Cooperation and Development have also jumped on board the data bandwagon. At the centre of this movement is the concern that the data contains intimate details of a person's private life which may be misused with potentially grave consequences. In the aftermath of the anti-government food protests in 2008, Egyptian

[11] Heinonen,Risto (2008) There is no privacy in the everyday Information Society at www.lib.eduskunta.h/dman/document.phpx? accessed on 12th August,2013
[12] Weigel, Margaret (2013). The State of Internet Privacy in 2013 : Research round up at www.journalistsresource.org/another/ margaret-weiget. Accessed on 5th Feb,2014

authorities obtained call and text messages held by the private sector to track down and convict protestors. As Alex Pentland, director of the Massachusetts Institute of Technology pointed out 'imagine what Myanmar Gaddafi would have done with this sort of data.

The revelations by Edward Snowden have brought to light that the fight ahead for privacy rights in the cyber world will be long and tough. The response of the US and UK governments to accusations of mass and invasive global spying programmes has been to seek to justify such invasions on the plea of national security. The HINDU in a report on September 9, 2013 under the title "Govt violates privacy safeguards to secretly monitor Internet traffic'' by Shalini Singh has revealed that in an investigation conducted by the newspaper, Internet activities of India's roughly 160 million users are being subjected to wide ranging surveillance and monitoring much of which is in violation of the government's own rules and notifications for ensuring ''privacy of communications.'' While the CMS or the Central Monitoring System project is in its early stages of launch, investigation by the HINDU has revealed that there exists without much public knowledge----Lawful Intercept and Monitoring (LIM) systems which have been deployed by the Centre for Department of Telematics (C-DoT) for monitoring Internet traffic, e-mails, web browsing, Skype and any other Internet activity of Indian users[13].

VI. THE INDIAN SCENARIO

In the case of the Indian government, the LIM system is deployed at the international gateways of large ISPs. The functioning of these systems are immune to interception by the ISPs and are under lock and key so as to be in the complete control of the government. 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 the government controls the LIMs, it directly sends software commands and sucks out whatever information it needs from the Internet pipe without any intimation and information to anyone except to those within the government who send the Internet traffic monitoring commands[14]. This monitoring facility is available to nine security agencies including the IB, the RAW and the MHA. The governments' monitoring system which is installed between the ISPs Internet Edge Router (PE) and the core network has an 'always live' link to the entire traffic which enables the LIM system to have access to 100% of all Internet activity with

[13] *Id.*
[14] Weigel, Margaret (2013). The State of Internet Privacy in 2013 : Research round up at www.journalistsresource.org/another/ margaret-weiget. Accessed on 8th Apr,2020.

 [ISSN 2581-5369]

broad surveillance capability based not just on IP or e-mail addresses, URL's, HTTPs, FHT pc, tele-net or webmail but even through a broad and blind search across all traffic in the Internet pipe using 'keywords' and 'key phrases.' In addition to LIM systems being installed, the Government of India runs the Central Monitoring System or CMS which is a clandestine mass telecommunications technology development centre and operated by Telecom Enforcement Resource and Monitoring (TERM) cells. This program also gives security agencies and Indian Income Tax authorities centralized access to the country's telecommunications network and the ability to listen in and record mobile, landline, satellite calls and voice over Internet Protocol (VoIP) and read private e-mails, sms and mms and track the geographical location of individuals all in real time.

It can also be used to monitor posts shared on social media such as Facebook, LinkedIn and Twitter and to track user's search histories on Google without any oversight by the Courts or Parliament. Senior Internet researchers feel that the CMS is chilling in view of its reckless and irresponsible use of the sedition and Internet laws. They feel that it may be used to silence critics, journalists and human rights activists. The right to privacy is guaranteed under the Universal Declaration of Human Rights and the International Covenant of Civil and Political Rights to which India is a state party. Article 17 of the Covenant provides that:

(i) No one shall be subjected to arbitrarily or unlawful interference neither with his privacy, family, home or correspondence nor to unlawful attacks on his honour and reputation;

(ii) Everyone has the right to the protection of the law against such interference or attacks.

For quite a long time in India there was no law governing cyber laws involving privacy issues, jurisdiction issues, intellectual property rights and a number of other legal issues. To optimize benefits of ICTs and secure confidence of user's information society should be safe and secured not only through cyber laws per se but also appropriate enforcement mechanisms. In order to formulate strict statutory laws to regulate the criminal activities in the cyber world the Indian Parliament passed the ''Information Technology Act, 2000"to protect the fields of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber-crimes. The Act was further amended in the form of Information Technology Amendment Act, 2008. The Information Technology act, 2000 contains a number of provisions which can be used to safeguard against online/computer related privacy. The Act provides for both civil and criminal liability with respect to hacking

 [ISSN 2581-5369]

(Sections 43, 66)[15], imprisonment for a period up to three years for electronic voyeurism (Section 66E), phishing and identity theft (66C, 66D) and offensive e-mail (66A). Section 72 A of the I.T. Act penalizes the unauthorized disclosure of personal information by any person who has obtained such information under a lawful contract. Besides these the Act also contains provisions with respect to data protection as enumerated below.

Section 43a of the IT Act 2008 asks corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable security practices' failing which they would be liable to compensate those affected by any negligence attributable to the failure.

Sensitive personal information includes:

- **a.** Password
- **b.** Financial information such as bank account, credit card or debit card details
- **c.** Physical, physiological and mental health conditions
- **d.** Sexual orientation
- **e.** Medical records and history
- **f.** Biometric information
- **g.** Any detail relating to the above clauses as provided to body corporate for providing service.
- **h.** Any of the information received under the above clauses by the body corporate for processing, storing or processing under lawful contract or otherwise.

Any corporate body is forbidden by the rules from collecting sensitive personal information unless:

- **a.** The information is collected for a lawful purpose connected with a function or activity of the agency and
- **b.** The collection of the information is necessary for that purpose.

VII. Conclusion

Richard A Spinello (2002) has wistfully said 'in ten or fifteen years we may look back to the abundant privacy we enjoyed at the inception of this new millennium.' According to him the slow evanescence of personal privacy is not likely to abate soon but the reasons for erosion of individual privacy are quite complex. It is true we may fall prey to the numerous dangers lurking in the grey world of Internet. But perhaps we ourselves are to blame for this as we fall

[15] Information Technology Act,2008

 [ISSN 2581-5369]

to the ambiance and comfort of shopping or chatting offered through the Internet. Our privacy is thus sacrificed at the altar of information technology for tangible and more immediate benefits because for us the concept of privacy has always been of an abstract and ineffable value. (Spinello, 2002) On the flipside, the technological revolution which is used to destroy our privacy can be used to protect it if we exercise some self-regulation. We may exercise caution while disclosing our personal details and should adopt technologies that offer safeguards for privacy protection. Though the onus lies on governments of various countries to formulate effective legislations for privacy protection, however, we may take adequate safeguards by utilising more privacy enhancing technologies.

*****

 [ISSN 2581-5369]