CYBER SPACE VIS-A-VIS RIGHT TO PRIVACY

Deepthi Arivunithi,
I Additional District Judge, Madurai.

The term 'right to privacy' could be taken to mean an individual's right to be free from intrusion or interference by others. Cyber space means a non-physical terrain created by computers[1]. Most often than not, in the recent times, citizens (also referred to as 'netizens') have been increasingly making use of the cyber space to seclude themselves from their social circle. There is a general belief that these people are private and want to secure their privacy. In reality, it turns out that there is a serious threat of infringement of privacy of an individual in the cyber space. This article is an attempt to compile the information gathered by the author in this regard.

In order to recognize digital evidence and electronic records, the Information Technology Act (hereinafter referred to as 'the Act') came into force on and from 17.10.2000. The preamble of the act would read as follows:-

> "*An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.*[2]"

1 Cyber space as defined in http://www.kmandco.co.ke/the-right-to-privacy-and-cyber-space/

2 Preamble to Information Technology Act, 2000

The Act also recognized few forms of cyber crimes and provided for punishments for the same. The cyber crimes made punishable under the Act are set out from sections 65 to 85. The punishment prescribed thereunder, ranges from imprisonment upto three years to imprisonment to life and any fine amount could be imposed. An upper ceiling limit ranging from Rs.1,00,000/- to Rs.5,00,000 is also prescribed.

The cyber crime is an evolving field and therefore with changing times, more and more crimes that emerge from violations committed in the cyber space is detected. The common forms of the cyber crimes have been broadly categorized into cyber crimes against person and cyber crimes against property. Since, the present article seeks to examine the rights to privacy of individuals, the cyber crimes against person is more relevant to the present topic.

The categories[3] of the crimes against persons in the cyber space could include

(i) Harassment via E-Mails: The said offence is one wherein the sender tries to harass the victim by sending emails, text, messages, pictures, videos, attachments and folders by way of harassing the victim.

(ii) Cracking: This offence is committed when the computer system of an individual is compromised without the knowledge of the victim and the confidential data is accessed without consent and is tampered.

(iii) Cyber-Stalking: This is a form of harassment, when the offender constantly harasses the victim through electronic means. The electronic means would include internet, e-mail, phones, text messages, webcam, websites or videos.

3 The categories of the crimes have been adapted from the article found in https://www.lawctopus.com/academike/cyber-crimes-other-liabilities/

(iv) Hacking: This is the most common form of crime that is known to the users of the cyber space. Hacking basically means taking complete control and access over the computer system and destroying the entire data that is available. Hacking could also be done over the telecommunication and mobile network.

(v) Dissemination of Obscene Material: This refers to the offence, whereby the offender exhibits material relating to indecent exposure or pornographic content or hosting prohibited content.

(vi) Spoofing: This basically refers to stealing of identity of a person. By stealing the identity of the victim, the offender will make use of the identity of the victim to communicate to third persons. It would appear as though the victim is indulging in such communication.

(vii) Page jacking: This is an offence, wherein the website of a victim is compromised and is used to link some other fake website. In effect, when a user clicks on the link of the website of the victim, he would be linked to the fake site. Thus, the search engines can be tricked to list the fake website.

(viii) Carding: The electronic magnetic field of the ATM cards including credit cards are stolen and are used by the offender to swipe off the money from the victim's account.

(ix) Other crimes: Any other crime like cheating, fraud, threat to life and other forms of crime punishable under the Indian Penal Code, when committed with the help of the electronic devices or by making use of the cyber space, it falls within the ambit of cyber crime against persons.

The commonly known forms of the cyber crime is set out herein above. It is to be noted however, that every act of infringement of privacy is not made a cyber crime. Therefore, irrespective of the above offences, there is need for awareness with respect to the privacy rights of an individual that is infringed in the cyber space. A few

instances of compromising the privacy of a person is set out hereinafter. The most common form of intruding privacy of an individual in cyber space is called spamming. All of us using the internet are always pleased with the capability of the web browser to remember the sites we have visited. Not many of us have given a thought to the fact that each and every page we visit on the internet is tracked. In the internet browser, there is an option for use of an incognito window. The same is also called private browsing. Though there are many persons using this option to prevent their browsing from being tracked by the others, they must have failed to notice the disclaimer put up on the window. Usually when the incognito mode[4] is selected there appears a message that most of us omit to read.

> "*The said message clearly specifies that the pages viewed incognito would not stick around in the browser history, cookie store or search history after you have closed the incognito window. However, any file you download or bookmarks you create will be kept. Further, the message also warns you that you are not invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider or the websites you visit.*"

There are many youngsters and other adults who prefer this option conveniently to hide their browsing details from the members of their family. Though the browsing history is not saved, often the users are perplexed when the internet service provider and the other websites visited send out a whole-lot of unwarranted messages by tracking the websites visited by them (both through ordinary browsing and through incognito web browsing). This is called spamming and usually the browser in not aware as to why the messages were sent to him. Therefore, what is required is awareness with regard to the effects of using the cyber space.

4 Use Chrome web browser or any other internet browser to select incognito mode and see the message that flashes therein.

Likewise, during chats and other conversations over the internet, persons share their personal details, which could be used by the tracking system. However, we remain blissfully ignorant of the fact and think that the details we share are only received by the intended recipient. It is also important to note that the information we share over the internet could be accessed by large number of people. This is especially crucial in the case of social networking sites where people share their personal information. Any unauthorized access to the personal information or misuse of information is likely to affect a person's right to privacy in a serious manner. To make matters worse the unauthorized usage may not come to one's notice until it is too late to repair the damage.

Another instance, which is worthwhile to quote is with regard to mobile applications. The downloading of mobile application is also currently the trend with the increasing use of smart phones. While downloading a new application, usually the application seeks permission to access[5], which is most commonly ignored. If time is taken to go through the permission it seeks, it will be easy to notice that certain applications will seek permission to access, modify and sometimes delete contents of your emails, SMS, and other personal files. If the same is accepted without applying mind, it could result in serious invasion of a person's private information. Thus, there is an imminent necessity to be better informed about the advantages and disadvantages of using cyber space. A person accessing the internet has to take time to read the terms and conditions, privacy policy, permission details etc. While using the social networking sites/applications, it is important to set proper preferences in the security set up. The individual must also be cautious while permitting access to personal information while downloading applications in mobile phones.

5 Go to google play store and select an application to download. Press download button and then immediately a small window opens with regard to apps permission.

Though, the present article seeks to highlight the privacy issues relating to cyber space, it is felt that the issue of privacy cropping out of digital communication is also relevant. The legislations with regard to the digital communications are only a handful. Already, the Information and Technology Act has been discussed. The other relevant piece of statute in this regard is The Indian Telegraph Act, 1883 which governs the use of wired and wireless telegraphy, telephones, teletype, radio communications and digital data communications. It gives the Government of India exclusive jurisdiction and privileges for establishing, maintaining, operating, licensing and oversight of all forms of wired and wireless communications within Indian territory. It also authorizes government law enforcement agencies to monitor/intercept communications and tap phone lines under conditions defined within the Indian Constitution. The act came into force on October 1, 1885. Since that time, numerous amendments have been passed to update the act to respond to changes in technology[6].

The Telecom Commercial Communications Customer Preference Regulations 2010 is one of the pieces of regulations, which prevents the service providers from arbitrary sharing of personal information. Access Providers as defined under the regulations include the Basic Telephone Service Provider, Cellular Mobile Telephone Service Provider and Unified Access Service Provider. Thus, all forms of service providers are included within the regulations and the licence holders have to act in accordance with the regulations prescribed therein. Thus, all the service providers have to take necessary measures to protect the privacy and information shared on their networks.

6 http://www.dot.gov.in/act-and-rules/indian-telegraph-act

The Hon'ble Supreme Court has also dealt with the right to privacy in the context of interception of phone calls in the case of Amar Singh v. Union of India[7]. The interesting question that came up for discussion before the Apex Court was with regard to the duty of the service provider, when a request is made to intercept calls. In this context it was observed as follows:-

> "*40. In view of the public nature of the function of a service provider, it is inherent in its duty to act carefully and with a sense of responsibility.*
>
> *This Court is thus constrained to observe that in discharging the said duty, respondent No. 8, the service provider has failed.*
>
> *41. Of course, this Court is not suggesting that in the name of verifying the authenticity of any written request for interception, the service provider will sit upon it. The service provider must immediately act upon such written request but when the communication bristles with gross mistakes, as in the present case, it is the duty of the service provider to simultaneously verify its authenticity while at the same time also act upon it. The Central Government must, therefore, frame certain statutory guidelines in this regard to prevent interception of telephone conversation on unauthorized communication, as has been done in this case.*"

In this case however, ultimately, finding lack of substance in the writ petition, the Apex Court dismissed the writ petition. However, the observation made with regard to the duty of the service provider marks the importance given to the right of privacy of an individual.

7 (2011) 7 SCC 69

The question, whether interception of telephonic message /tapping of telephonic conversation constitutes a serious invasion of an individual right to privacy was considered by Hon'ble Apex Court in detail in the case of People's Union case[8], wherein it was held as under:

> *"17. We have, therefore, no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law".*
>
> *18. The right to privacy -- by itself -- has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy".*
>
> *Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. It is considered so important that more and more people are carrying mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law."*

8 People's Union for Civil Liberties (PUCL) v. Union of India, reported in (1997) 1 SCC 301

In the case of State of Maharashtra v. Bharat Shanti Lal Shah and Ors.[9] the issue that came for discussion was the validity of certain provisions of the Maharashtra Control of Organized Crime Act, 1999. The said act authorized the investigating agency to intercept calls whenever found necessary as provided therein. The said act was upheld by the Hon'ble Supreme Court by holding as follows.

> "*44.The interception of conversation though constitutes an invasion of an individual right to privacy but the said right can be curtailed in accordance to procedure validly established by law. Thus what the Court is required to see is that the procedure itself must be fair, just and reasonable and non arbitrary, fanciful or oppressive."*

Thus, one cannot but notice, that the courts of law have also given considerable importance and emphasis to the privacy rights of an individual in respect of digital communications. The first step of the Government of India taken towards protection of rights of the common man in the cyber space is the National Cyber Security Policy – 2013, which was notified on 02.07.2013. The vision of the policy is to build a secure and resilient cyber space for citizens, businessmen and government. The mission is to protect the information and information infrastructure in cyberspace, build capacities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and co-operation. The objectives also indicate that there is a serious step towards establishing a foolproof system to combat the legal issues arising out of the usage of cyber space.

9 (2008) 13 SCC 5

To conclude, it is found that each individual accessing the cyber space ought to be better informed about the advantages and disadvantages of using the same. It is necessary to be a responsible user of the cyber space and awareness is the key. The law in respect to the right to privacy with respect to cyber space is still in its nascent stage and therefore, the individuals have a key role to ensure that their rights to privacy are not intruded due to ignorance.