Journal of Advances and Scholarly Researches in Allied Education

Vol. X, Issue No. XX, Oct-2015, ISSN 2230-7540

ROLE OF TECHNOLOGY IN INVASION OF RIGHT TO PRIVACY

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

Journal of Advances and Scholarly Researches in Allied Education
Vol. X, Issue No. XX, October-2015, ISSN 2230-7540

Role of Technology in Invasion of Right to Privacy

Sanjiv Shukla

Research Scholar, Maharaja Vinayaka Global University, Jaipur

Abstract – In the earlier times in India, the law would give protection only from physical dangers such as trespass from which the Right to Property emerged to secure his house and cattle. This was considered to be part of Right to Life. As the ever changing common law grew to accommodate the problems faced by the people, it was realized that not only was physical security required, but also security of the spiritual self as well as of his feelings and intellect was required. The strategy adopted by the Supreme Court with a view to expand the ambit of Art. 21 and to imply certain right there from, has been to interpret Art.21 along with international charters on Human Rights. Right to privacy is not enumerated as a Fundamental Right in the Constitution of India. In the context of Article 19(1) (d), the right to privacy was again considered by the Supreme Court in 1975. In the context of surveillance, it has been held that surveillance, if intrusive and seriously encroaches on the privacy of citizen, can infringe the freedom of movement, guaranteed by Article 19(1) (d) and Article 21. Surveillance must be to prevent crime and on the basis of material provided in the history sheet.

Keywords: Right, Privacy, Technology

----------X----------

INTRODUCTION

In present scenario people are more prone to privacy invasion due to the development of the internet. Once an individual posts something on the web, it stays on the web. Pictures, phone numbers, social security numbers, emails, work information, anything needed for fraud can be found on the web or through a company. Internet users post comments on Facebook or Myspace telling a friend to call them unknowingly leaving their number on that page. Users post their full names, date of birth, place of birth, pictures, and their place of residence. All this information adds up to a beautiful result to hackers and stalkers online. Hackers gather information about a person, sell it or use it to open new credit cards, buy expensive things, and rip people off with a false name. [Expand here about other internet issues]. Google and other search engines save everything typed on their websites from ones IP (Internet Protocol) address. Google has stated that no personal private information is stored however; topics come to debate evolving Google selling information to people. Ebay, Amazon, Paypal, and other pay sites pose a large threat to privacy on the web. Ebay and Amazon store user's credit card numbers online and has an auto-fill form on all auctions. Auto-fill forms are the brackets of information someone fills out and the website automatically inserts the answer every time that question is asked again.

We are currently living in the so-called information age which can be described as an era where economic activities are mainly information based (an age of informational). This is due to the development and use of technology. The main characteristics of this era can be summarized as a rise in the number of knowledge workers, a world that has become more open - in the sense of communication (global village/Gutenberg galaxy) and internationalization (trans-border flow of data).

This paradigm shift brings new ethical and juridical problems which are mainly related to issues such as the right of access to information, the right of privacy which is threatened by the emphasis on the free flow of information, and the protection of the economic interest of the owners of intellectual property.

Almost every day brings new revelations about how someone snoops on us and mines our online activities for profit. Even so, we are only beginning to understand the power of these incursions. In a few years, our faces alone, snapped on a street, in a crowd, or posted by a friend on the Internet, will be the key for a search engine to reveal the stories of our lives.

The advantage of using modern communication devices is that transfer of information is possible without confronting obstacles such as distance and time. At the same time, the possibility of information

or *data* being intercepted and being placed in the hands of unintended parties has also increased. It is for this reason that privacy has become an issue in the context of electronic devices, communication and data transmission. Therefore, the need for stringent laws protecting personal data cannot be understated. (Information Technology, 2000).

Are "Privacy" and "Data Protection" Two Distinct Concepts?

The meaning of privacy has already been dealt with. However, with view of answering the question as to whether privacy is a distinct concept from data protection it is first necessary to define *data*. One of the most comprehensive definitions of "data" is found in the Information Technology Act of India (in Section 2(o)).

Thus, data protection means the protection of information that can be generated using computer systems, as defined above (Privacy and Human Rights, 2001).

Privacy is generally said to have four aspects; which are namely: Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";

2. REVIEW OF LITERATURE:

Wiretapping – amounts to search

Katz v United States (1967): Charles Katz used a public pay phone booth to transmit illegal gambling wagers from LA to Miami & Boston. FBI recorded his conversations using an electronic eavesdropping device attached to the outside of the phone booth and Katz was convicted based on these recordings. He challenged his conviction, arguing that the recordings were obtained in violation of his 4th Amendment rights. SC ruled that amendment's protections apply only when the searched party has a "reasonable expectation of privacy" & in this instance Katz would have had such expectation. This case made wiretapping by state and federal authorities subject to the Fourth Amendment's warrant requirements

Phone tapping

People's Union for Civil Liberties (PUCL) v Union of India (DoJ: 18.12.1996):

Public interest litigation filed protesting rampant instances of phone tapping of politicians' phones by CBI; Right to Privacy held to be inherent in Article 21;

Explicit guidelines laid down for exercise of rights of interception under S.5 of Telegraphs Act, 1885. It may be apt to quote the words of Justice Kuldip Singh in this famous case concerning telephone tapping (Audio)

Amar Singh v Union of India (DoJ: May 11, 2011) (SC):

Petition filed invoking Article 21. Interim reliefs granted and in force for several years. Duty of service provider to exercise care and caution in complying with alleged orders for interception/wiretapping emphasized (People's, 1997).

The Internet

The internet is a network of networks linked with millions of computers worldwide for communication purposes. The internet is a medium through which people can access information stored in other computers linked to the internet.

Any computer connected to the Internet can access any other linked computer and *vice versa* (provided permission and necessary access is granted by the computer owners). For example, if A's computer is linked to the Internet and A wishes to share certain files in his computer with others, A may grant access to these files to other users of the Internet. A can also grant access to only one or a group of computer users by employing network restrictions. A can also prevent others from forcing access to A's computer by installing appropriate firewalls and Internet security software. Nevertheless, the very objective of the internet is to provide information access and sharing. This is a hacker's idea of heaven. Let us examine a few ways in which privacy can be breached through Internet usage (Reed, Angel, 2007).

The "Cookie" Crumbles

A cookie is not as sweet as it sounds. A cookie is a simple text file that will be discretely placed in the computer's hard disk when it gains access to certain websites. It stores information about the user. For example, it may store certain preferences shown by the user, such as: which part of the website the user frequently accesses; the time spent in these websites; or the user's preferred content. These are usually known as "click stream data". The methodology by which websites gather such information may be ascertained by reference to the ***Double Click* case**, which came up as a result of an investigation by the Federal Trading Commission (FTC), into allegations made by privacy advocates that Double Click, Inc. was indulging in restrictive and unfair trade practices within the meaning of the FTC Act of the United States.

Thus, websites can often record information of the user's preferences and adapt accordingly to suit the user. This is in a way convenient to users, but may become a menace if the websites trigger pop-up advertisements, which is an annoying experience for most users. Also, this may become a hazard to privacy

as the gathered information relates to the user's choices and preferences.

Of course, cookies can be disabled in Internet Explorer and Netscape Navigator. Yet websites that require cookies would not be accessible to the user in that case. Thus, as said before, "cookies" – at least in the *online* world are most certainly not as delicious as the cookies that are manufactured by our favourite confectioner. Cookies must not be misused and the usage of it for commercial advertising purposes must be strictly regulated.

The Web Bug: Not the Spider

The Web Bug is another mode in which user movements on the internet can be monitored. The methodology is to use images known as **GIFs** in the webpage to trace the movements of the Mouse and Cursors. Also, if sent with email, this can be used to determine if the email has been read by the recipient and if it was forwarded, and to whom it was forwarded. This can be a clear peep into one's individual privacy. A case that is illustrative of the damage that can be caused by the use of Web Bugs was the privacy litigation concerning **Pharmatrak, Inc**. (See)

3. SOCIAL NETWORKING:

Humans are social creatures. Over the years, IT has embraced almost every aspect of human life and has not failed to take into account the sociable quality of people. The social habits and behaviour of humans have been given an electronic facelift by the IT industry, giving rise to the concept of "social networking". However, the large volume of personal information that is fed into these Social Networking Sites (SNSs) by computer users poses a serious threat to individual privacy.

Thus, SNSs are an information heaven for potential computer criminals that prey on personal information found on the internet.Main law in India relating to Information and Computer Technology is Information Technology Act 2000, which was enacted to safeguard against cyber related crimes.

Due to continuous and exponential advancement in technology in the last decade, this act has been amended time and again to cater for graver cyber-crimes. But still many cyber-crimes are not covered and more importantly implementation machinery is very weak i.e. Police who has to file the FIR, is mostly unaware of IT Acts provisions. In view of it is felt that though this act is perceived to be a draconian act but is it really affective?

The Internet has had a massive impact on many areas of personal and professional life. Defamation laws and libel lawsuits are one such area and many individuals, businesses, and website owners have fallen foul of the belief that they can write anything about anybody when they are online. With the proliferation of social networking websites ("SNW") and their widespread use, especially amongst the youth, one observes certain legal loopholes in their operation and use. On the one hand, while such Social Networking Websites provide an easy to use, convenient and cost effective way of networking, however the flip side presents the drawback of such Social Networking Websites. One such glaring drawback is the opportunity they provide for "cyber-defamation".

The most commonly accepted definition of Social Networking Websites, can be described asweb-based services that allow individuals to

- Construct a public or semi-public profile within a bounded system,
- Articulate a list of other users with whom they share a connection, and
- And traverse their list of connections and those made by others within the system'. (In re Doubleclick Inc. 2001).

The popularity of Social Networking Site among school students gives rise to two distinct kinds of threats to privacy. The first set of concerns relates to the disclosure of personal information by the students themselves. The second set of concerns, on the other hand, relates to the posting of personal information about a student by other people, including the possibility of other people altering someone's personal information.

4. DATA COLLECTION BY PRIVATE BUSINESSES:

Growing technological capabilities have led to an imbalance between state regulation and market power of Internet enterprises. Recent enforcement action by data protection regulators has highlighted the problems associated with policing these companies. For example, Google has repeatedly violated European data protection laws by collecting wireless data acquired by their mapping cars which take pictures for Google's Street View Service. Only after increased pressure and legal action Google gave in to the German authorities and deleted the data.

Based on this analysis, he may highlight conceptual basis of the legal rule, principle or doctrine and may forward some proposals for reforms. He need not go beyond the discipline of law. While inquiry into social dimension of law or societal role of law, traditionally, falls in the domain of sociologists as it, invariably, involves a systematic look at, or discovery of,

functional aspect of law and/or 'behavioural pattern' of an individual or a social group in response to 'law'. A sociologist intends to explain the way law functions and/or to evaluate its role in bringing out the desired changes. Undoubtedly, both the discoveries require 'systematic' study of, and approach to, 'fact', legal or social as the case may be, following a well-set 'methodology'. Hitherto, however, in the Law Schools' orientation in research methodology has been aimed at familiarization of law students with researching of legal materials-Acts of Parliament/Statutes/Proclamations, decisions of (higher) Courts, (case) digests, writings of legal scholars, indexes, rules of interpretation of statutes, and the art of distinguishing and finding the ratio decided of a case (predominantly in common law jurisdictions). In other words, Law Schools, hitherto, has been giving emphasis on analytical legal research. Legal scholars, therefore, have not been able to evolve any specific methodology of their own for carrying out legal research. They do not have well-articulated research methods to employ and research methodology to follow in legal research. Sociologists, on the other hand, have developed and inherited a comparatively well-developed research methods and methodology for systematic investigation of social fact or behaviour. (Secure Socket Layer)

Furthermore, France fined Google the maximum sum of 150, 000 Euros for data protection violations in January 2014. As the maximum penalty is so low, it has been suggested that Google deliberately ignored the law calculating the fine as an expense on the way to expanding their business. Another well-known entity in the context of data protection is Facebook. The social media enterprise is in constant conflict with European data protection authorities over their data protection laws because of customer surveillance. In particular the "Like" buttons enable Facebook to track user not only on Facebook but also on any site which displays such a symbol. In essence, when a user sees a "Like" button on any site he can be sure that Facebook has received his IP address, thus potentially enabling the identification of a user. This is in clear violation of European data protection law as it allows Facebook to create personalized user profiles. Further technological advancements such as facial recognition provide for a steady flow of new challenges for regulators in Europe. (GIF)

Once such data is (illegally) collected it is generally accessible through the appropriate procedures by the EU member state agencies which previously would have not had neither the capabilities nor the legislative basis to collect and process such data. Thus a potential conflict can arise when data is collected (illegally without the customer knowing or legally by way of consent through the terms of service) by a private entity for commercial purposes and subsequently used by government agencies for their legitimate public security purposes. (Computers Infected)

The right balance between privacy regulation and data protection on one side and data security on the other is hard to achieve. Without giving up some degree of privacy, data flows on the internet cannot be secured. For example, Microsoft wanted to share information with its business partners and later with the public at large on its security feed. This feed provides real time information on attacks, botnets and other treats. (US District Court, 2002)

CONCLUSION:

One of the main content law concerns when it comes to publishing any biographical material about others is that any publication may have the effect of violating their privacy. Under Indian law, the right to privacy is not well-defined. Nonetheless, it has been recognised under **Article 21 of the Constitution of India** which deals with the 'right to life and liberty'— given that Article 21 lays in Part III of the Constitution, the right to privacy is effectively a fundamental right. (Schwartz, 2004. Computers Infected)

Law, as mentioned earlier, can be perceived as a normative science as it sets norms of human behaviour. Most of the times, it also plays a role of catalyst for bringing socioeconomic change. It is a means to an end. A systematic investigation of the first dimension of law (as a normative science), generally, falls in the domain of legal academia. A scholar of law, generally, undertakes a rigorous systematic analysis, exposition and critical evaluation of legal rule, legal principle, legal concept or doctrine (i.e. legal fact).

REFERENCES

A Denial of Service Attack involves launching huge volumes of e-mail or other messages (more than the target system can handle) from multiple locations, thus disabling the target.

Audio, visual or both.

C. Reed and J. Angel (2007). Computer Law (Oxford: OUP,) p. 332.

Computers infected with a "Backdoor Trojan" that listens for remote commands and carries out remotely controlled actions.

GIF, which stands for 'graphics interface format', is a de facto standard for graphic images on the web. The term 'web bug' was coined by Richard M Smith to refer to GIF files used to monitor internet use. Richard Smith's web bug FAQ is available at http://www.privacyfoundation.org/http://www.privacyfoundation.org/http://www.privacyfoundation.org/.

In re Doubleclick Inc. (2001). Privacy Litig., 154 F.Supp.2d 497 (S.D.N.Y. 2001).

Information Technology (2000). Act No 21 of India.

P. Schwartz, (2004). "Property, Privacy, and Personal Data" 117 Harvard Law Review, 2056.

People's (1997) Union of Civil Liberties v Union of India, AIR (SC) 568.

Privacy and Human Rights (2001): an International Survey of Privacy Laws and Developments published by the Electronic Privacy Information Centre, Washington DC, USA.

Secure Socket Layer is an encryption technology on the server that scrambles important data such as credit card numbers and order information when it is being.

Seehttp://www.microsoft.com/security/glossary.mspxhttp://www.microsoft.com/security/glossary.mspx.

US District Court, (2002). District of Massachusetts, Civil Action No 00-11672-JLT, 13 Aug 2002.