

## Privacy Issues on the Internet

Dhrumi Gada<sup>Å\*</sup>

<sup>Å</sup>Government Law College, Churchgate, Mumbai- 400020, India

Accepted 05 Sept 2014, Available online 01 Oct 2014, Vol.4, No.5 (Oct 2014)

### Abstract

*The whole of science is nothing more than a refinement of everyday thinking- Albert Einstein*

*Technological advances in the area of telecommunications have resulted in an explosive growth of the telecommunications industry. Along with this growth, there has been a corresponding increase in the number of internet users. It is expected to grow potentially in the next few years. In 1995, the estimated range of internet users was about 26 million. In 1998, about 150 million people had access worldwide, and the number had reached to approximately 513.41 million by the end of august 2001. Today the internet is probably the fastest, cheapest and perhaps the best means of communication and information. Anybody with internet access and basic knowledge about the working of the computer and internet can utilize it for further his/her ends. However, this 'wonder' technology also raises many concerns. Online privacy is one of the grave issues.*

**Keywords:** Science, technological, telecommunications, internet, information, privacy, grave, issues.

### 1. Introduction

In one sense, all human rights are aspects of the right to privacy.

The internet, by its very nature cannot be regulated in any way and thus could be a threat to national interest, intellectual property rights, individual privacy, etc. this article attempts to analyze the privacy concerns of an individual on the internet by discussing the threats to privacy and the conclusions in order to protect them on the net or as the popular term goes: 'Netizens'

### Privacy

Of all the Human Rights in the International Catalogue, privacy is perhaps the most difficult to define. In many countries, the concept has been fused with data protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy is seen as a way of drawing the line at how far society can intrude into a person's affairs. Probably one of the best definitions to 'privacy' has been put forth by Alan Westin, author of the seminal 1967 work *Privacy and Freedom*, as the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behavior to others.

The preamble to the Australian privacy charter provides that, A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy. Privacy is a key value which underpins

human dignity and other key values such as freedom of association and freedom of speech...Privacy is a basic human right and the reasonable expectation of every person. On-line privacy is more than a theoretical problem. It is a real issue impacting even fairly unsophisticated computer users.

A Pew Survey conducted in the united states of America from May 19 to June 21, 2000, found 54% of American Internet users 'very concerned' that personal information about them or their families would find its way to businesses or strangers. Not surprisingly, 86% of those respondents favoured an opt-in approach to internet privacy, under which no internet company could use such information unless expressly authorized to do so.

The pew survey found that 64% of internet users would provide personal information if necessary to access a website and that only 24% of internet users who know about cookies have configured their web browsers to reject them.

The issue of privacy has become a nemesis for advocates of the new technology. Activists, regulators, courts, local and international governments insist that the current internet model violates individual privacy rights too freely.

### The Right to Privacy

Privacy is a fundamental human right. It has become one of the most important human rights issues of the modern age. Privacy is recognized around the world in diverse religions. Nearly every country in the world includes this right in its constitution. The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights (UDHR). Article 12 of

\*Corresponding author: **Dhrumi Gada**

UDHR states: No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks on his honor or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

Numerous international human rights treaties specifically recognize privacy as a right.

Let us analyze the right to privacy in the Indian Context:

Part III of the Constitution of India enumerated the Fundamental Rights guaranteed to a citizen of India. However, it does not expressly deal with the right to privacy. But due to judicial activism, the right to privacy is now an implied right under Article 21 of the constitution, which guarantees right to life and personal liberty. In *Unni Krishnan v. State of A.P.*, the Supreme Court stated that several unenumerated rights fall within Article 21 of which right to privacy is one.

Article 21 is of the widest amplitude. The Supreme Court in *Karak Singh v. State of U.P.* held that domiciliary visits by the police without the authority of law were violative of Article 21 assuming that right to privacy is derived from Article 19(1) (d). It referred to the American case of *Wolf v. Colorado*, where Frankfurter J. said the security to ones privacy against arbitrary intrusion by the police.... is basic to a free society.

Justice Subba Rao while quoting Frankfurter J., said that we would therefore define right of personal liberty in Article 21 as a right of an individual to be free from restrictions or encroachments on his person, whether these restrictions are directly imposed or indirectly brought about by calculated measures. It is true that our constitution does not expressly declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty. Right to Privacy may also be derived from Art 19(1) (d). Subba Rao J. also observed that Art 19(1) (d) is not mere freedom to move without physical obstruction but movement in a free country i.e. in a country where the citizen can do whatever he likes, meets whomsoever he wants to meet without any apprehension and a person under the shadow of surveillance is certainly deprived. Further, the Supreme Court, in *R Rajgopal v. State of T.N.*, Reaffirmed that the right to privacy is implicit in right to life and liberty under Article 21. Thus the right to privacy has now become an inseparable part of Article 21 and it ensures protection against arbitrary police intrusion.

The infringement of privacy has also become actionable in torts. The concept of trespass includes any direct invasion of a protected interest from a positive act which is actionable subject to a justification. If the interference to privacy is such as to amount to a recognized tort, then tort action may be taken to prevent the interference. For example, harassment by persistent phone calls may amount to a nuisance, and installation of a secret eavesdropping device may amount to a trespass. The High Court of Bombay has held that an invasion of privacy is an actionable wrong.

### Threats to Privacy

With the increasing use of internet in daily activities and

the amount of information collected by websites, the internet poses a grave threat to individual privacy. Whether it is the electronic surveillance carried out by governments to track political opponents and belligerent student dissident leaders, or a person who shops on-line, or an employee who accesses an e-mail service through the office network, they all are tracked for their online activity. Today's technology has made George Orwell's prophetic Big Brother's watching you come true.

### The various threats are as under

#### *State Surveillance*

The governments of various nations have always tried to prevent any kind of opposition against them. With the internet, the task of these authoritarian governments has become easy. According to a 1997 report, *Assessing the Technologies of Political Control*, commissioned by the European commission's Science and Technology Options Assessment Office (STOA), much of the internet technology is used to track the activities of dissidents, human rights activists, journalists, student leaders, minorities, trade union leaders, and political opponents. The report concludes that such technology (which it describes 'new surveillance technology') can exert a powerful 'chilling effect' on those who 'might wish to take a dissenting view and few will risk exercising their right to democratic protest.' The State surveillance has gained special importance especially after the September 11 attacks.

The latest in State surveillance created for the United States Federal Bureau of Investigation (FBI) is the controversial 'Carnivore' software. This software enables the enforcement agency to monitor and intercept all e-mails and browsing on the net. It places a computer running Windows NT at an Internet Service Provider (ISP) and can access and monitor all traffic about a user including e-mail and browsing. According to press reports the 'Carnivore' 'can scan the thousands of e-mails a second' and 'would give the government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web Surfing'. Such kind of surveillance system and high speed links to the Federal Security Service which would allow it direct access to the communication of the internet users without a warrant.

Further nations like the United Kingdom have enacted laws, which allow the intelligence office interceptions at any ISP. A number of countries are also demanding that ISPs install 'black boxes' on their systems that can monitor the traffic of their uses. The actual workings of these black boxes are unknown to the public. What little information has been made public has revealed that many of the systems are based on 'packet sniffers' typically employed by computer network operators for security and maintenance purposes. These are specialized software programs running in a computer that is hooked into the network at a location where it can monitor the entire data stream searching for key words, phrases or strings such as net addresses or email accounts. It can then record or retransmit for further review anything that fits its search

criteria. In many of the systems, the boxes are connected to government agencies by high-speed connections.

#### *Electronic Commerce*

Surveillance by the enforcement agencies is not the only way online-privacy can be infringed. The growth of e-commerce on the Net has increased the amount of personal information collected by individuals and corporations engaged in e-commerce. Some corporations are involved in sending unsolicited mails (spam) to consumers who surf their websites, while others give the information collected by them to third parties. This online profiling of the internet user has become an important aspect in e-commerce. All this is possible due to a trafficking called the 'cookie'.

When a website is visited, the server can write a file onto the user's computer hard-drive which characterized what took place at the site. A cookie is a small text file, which is sent by a website to be stored on the hard drive of the visitor. In general, cookies allow sites to 'tag' their visitors with unique identifiers so they can be identified each time they visit. It contains the preferences of the visitor, example the number of times the site has been visited by that particular computer and the services used repeatedly by that computer user. It also allows the owner of the website to view what took place at the website. Shopping basket cookies assign an identification value that remains constant as the user moves throughout he sites and saves all selections to a file corresponding to that identification values. Trafficking cookies, used primarily by direct marketing companies, assign an identification value the first time the user visits a site on which the company displays a banner ad and thereafter keep track of the other sites visited by the user assigned that value.

The cookies may infringe privacy in two aspects. First when the website has been visited, the cookie of that website can be accessed later and further the cookie file may reveal the other websites visited during that time frame. The second way in which the cookies infringe privacy is when the websites with the help of the cookies identify the Internet Protocol address through which the exact location of the computer used to access the website is identified. Thus the website can actually store personal information of an individual without the consent and the knowledge of the user. When this information, which is very important for e-commerce websites, is sold to these websites it will greatly undermine the privacy of an individual.

The above threat is only related to net-surfers. These are websites accessed through what are called 'Members Only' website. These websites offer online services for a payment of subscription. These websites can be subscribed online and the payment may be done through credit cards. They have a standard online subscription form which collect details such as the name, address, telephone number, and most important, the credit card number of the subscriber. Though these websites have a 'privacy policy' which guarantees non disclosure of the confidential information, they seldom abide by it. These websites if not regulated, can result in immense distress to the user.

Not satisfied with cookies which can be rejected or deleted by a user, the industry is also now developing more

permanent methods of identifying users. One of these is the use of web bugs, invisible images that also place cookies on users' computers, and a serial number for each chip which can be accessed by a website.

#### *Workplace Monitoring of Employee's email*

According to preliminary data from the American Management Association, as of the first quarter of 1999, nearly 30% of major U.S. companies currently monitor their own employee emails. Most of the firms have their own networks, which the employees use for personal as well as business purpose. If the monitoring of the emails of the employees is for the purpose of business, then the privacy of the employee is not infringed. But if the corporation accesses any personal email of an employee then there is sufficient cause for an infringement, assuming that an employee has a reasonable expectation of privacy and there is no ban on personal use.

#### *Hacking*

Though hacking itself is illegal in almost all countries, it poses the greatest threat to privacy. Hacking is an unauthorized intrusion into the computer system of an individual or an intrusion into a website's to source code so as to alter or access any data or information or a program posted on the website or in a particular computer. Hacking has led to tremendous monetary loss for the corporation and individuals.

#### *Legislations for privacy*

Registering for an on-line service or purchasing goods on the internet may require the disclosure of a wide variety of personal information, including name, age, address, credit card numbers and medical information. Consumers should be wary that information, very private, is readily collected, analyzed and used by cyber enterprises.

As a result, protection of personal information online has become a significant concern to legislators.

In India, till recently there existed no legislations relating to the internet. However, after the telecommunications boom in 1999-2000 pursuant to the New Telecom Policy, 1999 (NTP-99), the government found itself in an urgent need for regulating the fields of information Technology. This need for regulations paved way for The Information Technology Act, 2000. It is basically aimed at regulating online commercial activities. The Act as of now is the only legislation enacted by the Indian Government which deals with the internet. However, the Act does not substantially protect an individual's right to privacy on the internet. Even though the privacy issues are not given much importance amongst the Indian public, the law makers definitely have to gear up to find ways in which this growing concern can be combated.

#### **Conclusion**

Although nations around the globe have granted their citizens their right to privacy, they have not been able to

formulate effective legislations for the protection of online privacy. Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in protections. This grave issue needs immediate attention.

For that, there should be a limit on the collection of personal data and should be collected by lawful and fair means. It should be used only for the purposes they are meant to be used and the reason of this collection should be specified beforehand. In any case personal data should not be disclosed, or made available or accessed for any other purpose as specified above (except accessed by the authority of law). The body or institution or agency, collecting such data should safeguard personal data against such risk as unauthorized access, destruction, use, modification of data. The process of collecting data should also be very transparent and there should be a general policy of openness about developments, practices and policies with respect to personal data. An individual should have the right to access his/her data from the data controller. Furthermore, a data controller should be made accountable for complying with measures which give

effect to the principles stated above. The safeguarded flow of personal data should be promoted so every individual can enjoy its right to privacy in the most lucrative manner, because ... Privacy is a key value which underpins human dignity.

## References

- Mark S. Ditcher Electronic interaction in work place, [www.morganlewis.com](http://www.morganlewis.com)
- Rachel Zimmerman What are cookies?
- Simone Dvis (July 11, 2000) Big brother, [www.bigbrotherinside.org](http://www.bigbrotherinside.org) FBIS's system wall street journal.
- Science and technology option assessment (STOA), [www.privacyinternational.org](http://www.privacyinternational.org)
- Judgements and cases, [www.indiankanoon.com](http://www.indiankanoon.com), [www.manupatra.com](http://www.manupatra.com)
- 1948 Universal Declaration of Human Rights, [www.un.org/overview/rights.html](http://www.un.org/overview/rights.html).
- John Awerdick On line privacy, [www.cla.org/ruhbook/chp4.htm](http://www.cla.org/ruhbook/chp4.htm)
- Alan Westin Privacy and freedom, page 7
- Volio Fernando, Legal Personality, privacy and the family
- The Australian Privacy charter, <http://www.privacy.org.au/About/PrivacyCharter.html>