International Journal of Academic Research
ISSN: 2348-7666; Vol.3, Issue-4(1), April, 2016
Impact Factor: 3.075; Email: drtvramana@yahoo.co.in

Digital Privacy and Human Rights Protection in Cyber Space

Md.Sameera, JKC, PRR & VS Govt. College, Vidavaluru, SPS Nellore Dist.
I.S.chakrapani, *IQAC Coordinator, PRR & VS Govt. College, Vidavaluru, SPS Nellore Dist.*

With the widespread use of internet, the world has transformed into a global village. As the number of netizens is increasing, ample opportunities have been created. With E-commerce, e-governance, e-learning etc., virtual space is the home for much activity that encompasses the daily life. World has become an information society, for which communication is central. Ideally, no one should be excluded from having the benefits of accessing the World Wide Web. But in reality there is a digital divide affecting many countries. Digital equity is still a distant dream. Issues of national security are also of concern involving data flow and the State intervention is necessary to safeguard the rule of law. The State has an obligation to protect human rights also. To strike a balance, the State has to act diligently. Consequently digital privacy rights are at stake due to surveillance and profiling of internet users. Internet Service Providers (ISPs) and search engines collect anonymous data about internet usage, often involving human rights violation. There has been a good debate on the international arena about internet and human rights. As the largest democracy and one of the largest internet user bases in the world, India can play a crucial role in shaping up the debate and outcome. In this paper, we discuss the digital privacy issues and the international debate, and propose multistakeholderism as a remedy.

Key Words: Human rights, Digital privacy, ISPs, Profiling, Multistakeholderism.

Introduction

Cyberspace is identified with a domain encompassing the digitalized information, as well as the infrastructure, server networks, computers and the internet. The term 'Cyberspace' does not have a universally accepted standard definition. Cyberspace can well be defined by how it is used and can be identified with the World Wide Web [1].

Contemporary lifestyle includes accessing and transmitting information through the World Wide Web, which has progressively developed into a global community, wherein the individual citizen has the ability to connect with others without any political, social and racial borders [2]. Cyberspace is often considered as a domain in which the individual may find, develop and exploit their own 'parallel reality' [3].

The perception of cyber space has changed for the past four decades due to an overt inflow of information and literature. The concept of 'global common' has shaped itself as a result of awareness about the right to information as a social and human right. This concept, by its nature, includes all those goods and rights which are not suitable for appropriation by any individual, firm or State [4].

'Virtual reality' has contributed to the idea that cyberspace is not marked by any State control or governance. People all over the world have started to

think that within cyberspace, exchange of information and knowledge should be free and unconstrained by the rule of law, hence the 'Open access' movement.

It is often suggested that cyberspace is a non-physical realm and has no restricting boundaries. But in reality, the phenomena happening in cyberspace are linked to a clear geographical dimension. This dimension is represented by the server location, point of access, human conduct and a legally appreciable effect [5].

Human rights, equity and digital privacy in cyber space:

The United Nations World Summit on the Information Society (WSIS) was convened in December 2003. This was aimed at stimulating action to ensure that the information societies are more equitable than their predecessor. In this summit, considerable debate was around the core issue of human rights and their legal protection in digital spaces. The WSIS emphasizes a common vision with respect to human rights. The WSIS Declaration of Principles emphasizes that everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers [6].

Ideally, information society is expected to be inclusive. The ability to contribute must be fostered, besides providing access to information and communication. Strengthening the trust framework, including information and network security, authentication, privacy and consumer protection is a prerequisite for the development of Information Society. Reduction of 'digital divide' of many different kinds must be ensured [7].

The right to freedom of expression is often contained in many countries including India, due to incidence of defamatory speech in various social media. Internet mediated speech raises issues of standards to be applied and liability to be imposed whether on the originator, or an Internet Service Provider.

The use of digital technologies to provide and exchange information about prostitutes and /or pornographic materials is of concern. While human rights are being recognized worldwide and legal and socioeconomic solutions are being devised to protect women from exploitation, there is little recognition that civil and political rights are 'gendered' [8]. Intense agility of virtual pimps is so threatening that children's rights are severely infringed. Shocking is the fact that there are internet based communities to protect pedophiles and their activity.

The choices and actions of people using the digital technologies have raised concerns over safeguarding the rule of law and national security as such. The market for these technologies has grown considerably, but they raise crucial issues about the nature of 'public sphere' and about censorship. In view of misbehavior online that threatens harmony in the society and national integrity, state intervention as a form of governance involves human rights issues at times. Filtering information online, denying access and profiling of end users are common practices which at times may lead to strangulation of the open internet. This suggests that new technologies do not always support the empowerment of civil society movements [9].

Today's information societies are underpinned by digital technologies globally and locally. Ubiquitous networks are at the heart of this digital age. World Wide Web has an enormous repository of information and the internet is limited only by the limits of human imagination. Within the digital spaces, there are ample opportunities for development and these should be evenly available to all the people and all the nations. It's a pathetic truth that there has been a digital divide already established. The unevenness of access to the means of communication using digital technologies and the extent to which measures to be taken to reduce the effect of digital divides is an ongoing debate [10,11,12].

Cyberspace raises many issues for privacy protection. The individual's autonomy to decide what must be kept in the private sphere is often emphasized as a human right, amidst social apprehensions. It is of debate whether to consider transparency as a social right or not. Privacy infringement is often the result of data protection legislations that lead to surveillance and profiling, which concern many issues like nationality, race, ethnic origin and apartheid etc.

An increasing portion of daily life is being spent online by many people. While doing so, they leave a permanent digital footprint with every Google search, Face book 'like' and a Twitter 'tweet' and the like. This e-disclosure of self-identity & activity and its cumulative effects over time are much ignored by many people. Though they rail against data theft and allied crime, many of the most vigilant netizens even do not know the privacy violations that take place unseen and unheard online.

Privacy is enshrined in the United Nations Universal Declaration of Human Rights. These days, digital privacy has emerged as an important human right because it may be subjugated easily. Privacy is a guarantor of human dignity, important to maintain personal security, protecting identity and promoting freedom of expression in this digital age. It is unfortunate that many legislative priorities largely appear to exclude digital privacy. Many legal provisions evolving in the backdrop of overt terrorist activity across the world are perceived as overstepping of authority. This is in particular true with the collection, retention and analysis of personal data. Many of the products offered by leadership companies including encryption, endpoint protection, online backup and antivirus software support the United Nations Guiding Principles on Business and Human rights. But, it is true that many companies like Google, Yahoo and Microsoft store increasing amount of third-party personal and commercial data that may be of legitimate interest to governments and law enforcement agencies. There are incidences that companies provide personal data to comply with the local law may experience unintended human rights violation. This is also happening in many countries.

How to ensure safe and secure internet:

Ensuring safe and security in digital spaces can be guaranteed by three ways.

Governments and business firms should follow **cyberethics**, which are norms and principles that guide to steer internet governance, take decisions about the internet architecture, and to the behavior of end users. In order to ensure

safe, secure and tolerant internet, mutual respect for human rights must be emphasized and taught. Governments across the world impose restrictions that urge internet users to be more accountable and responsible in the context of debates around freedom of expression. For example, Freedom of speech and expression is protected by article 19 (1) of the constitution of India, but under article 19(2) "reasonable restrictions" can be imposed on freedom of speech and expression in the interest of "the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence"[13].

While restrictions are legitimate in some cases like those of hate speech, accountability on the part of all stakeholders is required to ensure the interlocking of rights and responsibility. Responsibility and accountability on the part of governments and businesses is also the dire necessity.

The issue of **cybersecurity** mixes together a number of debates, from cybercrime to national security through critical internet infrastructure. In the context of national security, surveillance is upheld as a solution. But surveillance and security contradict each other. It should be taken care that surveillance does not exploit the very vulnerabilities which should be patched to make internet secure. If safety is really a concern, it should be ensured that human rights are protected before we actually move to the cyber ethics frame work.

In addition, above all, **multistakeholderism** is essential. This is a matter of democracy, not of ethics. During the past few years, a strong push on internet governance can be observed. Governance of the internet is guided by government interference based on the traditional ideas of sovereignty. But it should be remembered that internet is a global network and owned by private actors and not by governments. So, the environment and the architecture by which internet functions is quite different from what we experience offline. Hence, checks and balances that we know offline do not work anymore in the context of internet usage. It is by bringing together all the actors on internet together, balance between national security/solidarity and human rights in cyberspace can be achieved. This is where multistakeholderism comes in safeguarding digital privacy in tune with national solidarity.

Internet governance must be about shared decision-making. This is a pivotal aspect of multistakeholderism and not mere consultation. The joint participation and decision making at every step of the process is required. This implies that simply one body at the United Nations or elsewhere is not sufficient. One process is not sufficient to resolve all internet related problems. A multitude of process is required, which is determined by the issue at hand. So to conclude, human rights and multistakeholderism must be linked together, so that we can move from internet to equinet.

References:

1. Maj.Gen. Mark Barret, Dick Bedford, Elizabeth Skinner & Eva Vergles. 2011, *Assured Access to the Global Commons, Supreme Allied Command Transformation*, North Atlantic

Treaty Organization, Norfolk Virginia, USA. p.35.

2. Vittorio Fanchiotti and Jean Paul Pierini. 2012, I*mpact of Cyberspace on Human Rights and Democracy,* 4th International Conference on Cyber Conflict. NATO CD COE Publications, Tallinn. Pp 49-60.
3. *Ibid.*
4. *Ibid.*
5. The Explanatory report to the European Cybercrime Convention, adopted on 8th November,2011 at Budapest, CETS/SEV No.185.
6. World Summit on the Information Society. 2003. *Declaration of Principles,* WSIS-03/GENEVA/DOCE/4-E, 12 December at http://www.itu.int/net/wsis/documents/HLE.html accessed on 16.11.2015
7. World Summit on the Information Society. 2003. *Plan of action,* WSIS-03/GENEVA/DOCE/5-E, 12 December at http://www.itu.int/net/wsis/documents/HLE.html accessed on 16.11.2015 accessed on 17.11.2015
8. Robin Mansell. 2009. *Introduction- Human Rights and Equity in Cyberspace*. Available at http://eprints.lse.ac.uk/3707/ accessed on 17.11.2015
9. Surman, M. and Reilly, K. 2003. *Appropriating the internet for Social Change: Towards the Strategic Use of Networked Technologies by Transnational Civil Society Organizations.* New York: prepared for Social Science Research Council.
10. Couldry, N. 2003. *Digital Divide or Discursive Design? On the Emerging Ethics of Information Space.* Ethics and Information TEchnolog, 5, pp.89-97
11. DiMaggio, P. and Hargittai, E. 2001. *From the Digital Divide to Digital Inequality: Studying Internet Use as Penetration Increases.* Princeton: Working Paper No.15, Center for Arts and Cultural Policy Studies, Princeton University.
12. Mansell, R. 2001. *Digital opportunities and the Missing Link for Developing Countries.* Oxford Review of Economic Policy, 17(@), pp.282-295
13. The Constitution of India, accessed from http://lawmin.nic.in/coi/coiason29july08.pdf on 17.11.2015.