

E-COMMERCE - SETTING GLOBAL STANDARDS IN INTERNET ADVERTISING

Sameer Joshi

Research Scholar, Shri J. J. T. University, Jhunjhunu, (Raj), India
Email: sierra1506@hotmail.com

ABSTRACT

Cyber laws are meant to set the definite pattern, some rules and guidelines that defined certain business activities going on through internet legal and certain illegal and hence punishable.

The E-commerce industry carries out its business via transactions and communications done through electronic records. It thus becomes essential that such transactions be made legal.

Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space. India is the 12th nation in the world that has cyber legislation apart from countries like the US, Singapore, France, Malaysia and Japan.

The business world is complicated and advertising is one of the most convoluted parts of the business often involve advertising. This is because the law is very fluid in this area, and businesses have to defend attacks from many collateral sources. When your business comes up with a new idea, you must protect it against infringing competitors and zealous regulatory agencies alike.

In such cases it becomes very imperative to study both the Laws of the land as well as the laws of that country in which the product/service is being advertised and marketed.. Many concepts are governed by such statutes.

Many of us may have experienced these when accessing our own e-mails. That's a great promotional idea but the campaign should comply with both the state and federal advertising law.

If India doesn't want to loose its position and wishes to stay as the world's leader forever in outsourcing market, it needs to take fast but intelligent steps to cover the glaring loopholes of the Act, or else the day is not far when the scenario of India ruling the world's outsourcing market will stay alive in the dreams only as it will be overtaken by its competitors.

Keywords: Cyber Laws, E-Commerce, World Wide Web, Advertising, Outsourcing.

OBJECTIVE

- The objective of this paper is to give an outline on introduction of new and innovative programs to promote better products and services in the field of Internet Advertising and Marketing.
- List out the legal perspectives corporates, advertisers, the hosts, consumers etc, should take into consideration with the Internet as the media.

INTRODUCTION**Global Standards & Competition**

In today's business environment most organizations face difficulty to develop an e-business strategy. Major changes that could be expected out of implementation of the new e-business strategy:

1. Improved ability to link and enable employees and codify the organization's knowledge base.
2. Improve boundary spanning capabilities and improvisation in information processing leading to better efficiency.
3. Improvisation in collaboration and co-ordination that promote innovation.
4. Creation of opportunities to establish interactive relationships in B2B and B2C transactions and Improvisation in Customer Service and strengthen Back-Office integration.
5. Creation of competitive advantages by providing new avenues and opportunities to cooperate and compete with their competitors thus creating new business avenues within the company's existing business line.

Global Standards in B2B and B2C Internet Based Marketing and Promotion**FTC Compliance Guidelines concerning Internet Advertising and Affiliate Marketing**

Addressing consumer privacy interests, the Federal Trade Commission ("FTC") on 1st December 2010, released a comprehensive report which raised concerns that despite industry self-regulatory measures, many marketers either do not disclose their data practices or disclose them in an unintelligible manner. FTC Chairman Jon Leibowitz said, "The FTC wants to help ensure that the growing, changing, thriving information marketplace is built on a framework that promotes privacy, transparency, and business innovation and consumer choice".

FTC Guidelines concerning Children's Online Privacy Protection Act [COPPA]

The FTC also has sought details on the review of its Children's Online Privacy Protection Act (COPPA) Rule. COPPA imposes requirements on operators of Web sites that are aimed at children under 13, and collecting their personal information. The rule requires online operators to get parental permission before collecting, using, or disclosing personal information from children.

The guidelines now impose liability on: (1) The advertisers, (2) The advertising agencies, and (3) The Endorsers (including celebrity endorsers). Further, the advertisers will be responsible for the claims made by endorsers.

Advertising & Communications Law

The more successful an advertising campaign becomes, the more likely the increased exposure could ultimately lead to a lawsuit. The fact of the matter is, when marketing of a product or service is legally challenged, the reputation of the products and services is also put on the line as well. In many cases, an advertising dispute is best resolved outside of court

which is often less expensive and less formal and in many cases work faster than the courts. Internet marketing is often surrounded in these legal grey areas.

Intellectual property concerns

This is an important aspect beyond the previews of the existing acts/ law and needs to be addressed as immediate concerns for standardization.

New Privacy Policy

A New Private Policy should be in place as there is a generalized opinion that nothing is private when information is disclosed on the Internet.

Example: The Face book privacy policy has grown from 1,004 words in 2005 to 5,830 today. Face book user now needs to click through more than 50 privacy buttons with more than 170 options in order to opt out of full disclosure of his or her personal information. Face book's privacy policy word count not only has eclipsed the US Constitution, it has also passed other major social networks such as Flickr (384 words), Twitter (1,203), Fraudster (1,977), and MySpace (2,290).

Security Measures

Computer "security" is the conceptual ideal which can be attained by the use of the three processes: Prevention (User account access controls and cryptography), Detection (Intrusion Detection Systems (IDS's) and Response.

Most current real-world computer security efforts focus on external threats, and generally treat the computer system itself as a "Trusted" system. Some knowledgeable observers consider this to be a disastrous mistake, and point out that this distinction is the cause of much of the insecurity of current computer systems.

Though India is the 13th nation in the world that has cyber legislation apart from countries like the US, Singapore, France, Malaysia and Japan, The IT Act 2000, even with the Amendments of 2008, still appears to be insufficient, and it takes mixed stand when it comes to many practical situations.

Deficiencies and Lacunas in The IT Act 2000 with Amendments of 2008

1. Internet is a borderless medium, and nobody knows how to enforce this Act all over the world at the same time???
2. The law misses out on important issues like Intellectual Property Rights, Entertainment Law, Copyrighting, Trademarks, Patenting of electronic information and data. The law even doesn't talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.
3. The law is silent over the regulation of electronic payments gateway and segregates the negotiable instruments from the applicability of the IT Act, which may have major effect on the growth of e-commerce in India. It leads to make the banking and financial sectors irresolute in their stands.
4. Now an officer in the rank of Police Inspector is empowered to investigate and file charge sheet in any case of cyber crime. This section is likely to be misused in case of Corporate India as companies have their offices in the metros and semi-metro cities, which come within the ambit of "public place" under the Act. As a result,

these companies will have to face harassment at the hands of the Investigating Officer in case of a crime committed.

CONCLUSION

1. The cyber laws of the country are regarded as insufficient and insecure for Indian e-commerce industry. Acceptance of this Act world-wide would be a difficult assignment as there are very less number of countries who have come together with a common agenda.
2. If India doesn't want to lose its position and wishes to stay as the world's leader forever in outsourcing market, it needs to take fast but intelligent steps to cover the glaring loopholes of The IT Act with its Amendments.
3. Setting Global Standards in Internet Advertising across the world is difficult as there are differences in culture, language, individual laws of respective countries, and need to set up an International Body on the lines of WTO, NATO, UNSC etc, to take up cases of organized Cyber Crimes and preventions across the world.
4. Setting up respective offices in order by way of adequate security systems, Firewalls, and "TRUSTED" Administrators will be beneficial for the companies to restrict employees from committing frauds.
5. Every sensible individual should take an oath not to fall prey or become victims of Cyber Crimes.

REFERENCES

1. W.R. King, IS Strategic Planning- Information Systems Management, 2000.
2. G.S. Kearns, Journal of Strategic Information Systems, 2000.
3. Lederer, A.L. Mirchandani- Search for strategic advantage from World Wide Web-2001.
4. Futla, F. Dhaliwal, Electronic Networking Applications & Policy, 2002.
5. Federal Trade Commission Guidelines Report, December 2010.
6. Amendments of 2008 to The IT Act, 2000, Dr. Sanjay Tungar - Cyber Cell, Pune.
7. Implementation of Amendments of 2008 to The IT Act 2000, Cyber Crime Cell, Satara.