



Cyber Laws For CxO

Be Aware... Be Empowered

January 2010

Editor

Naavi

www.naavi.org

Publisher

Ujvala Consultants Pvt
Ltd

www.ujvala.com

Since October 27, 2009, India has entered a new Cyber Law regime with a focus on Information Security and compliance.

This unique news letter tries to bring to the desks of CxOs, the latest developments in Cyber Laws affecting the management of business along with a knowledge update on selected themes.

The theme of this inaugural issue is "Intermediaries and their responsibilities under Cyber Laws of India".

Theme

**Intermediaries and their
responsibilities under ITA 2008**

In This Issue

Editorial: Empowerment of CxOs

Knowledge+: The Compliance Dilemma of an Intermediary

News Snippets: Seeds of Cyber World War.. and others

Interviews: Dinesh Pillai, Mahindra SSG: Rajat Mohanty, CEO, Paladion

Messages: Rakesh Goyal, Editor CCC Times, Ravi Jagannathan, CEO, E-Mudhra, Rakesh Nag, IIMA and Cyber Law Student

Questions and Answers

Archived Issues will be available at
<http://www.cyberlaws4cxo.com>

Editor's Note



Over the last decade, globally IT laws have tended to mandate compliance and the CxOs were slowly getting drawn into integrating “Regulatory Compliance” as part of the business strategies. However, In India Information Technology Act 2000 (ITA 2000) largely remained unnoticed by the corporate world until substantial amendments were passed with effect from October 27, 2009.

With these amendments, the new version of ITA 2000 which is referred to as ITA 2008 has now made all CxOs sit up and take notice of the existence of this Act which has introduced many mandatory Information Security practices. Compliance of these provisions has now become the responsibility of the top management of every corporate entity in India.

Additionally, the operation of Clause 49 of the SEBI listing guidelines, has thrown a critical challenge to listed companies to append a certificate in their annual reports that “all regulatory compliance requirements have been fulfilled”. The Directors of the Company including the “Independent directors” will now be responsible for the regulatory compliance and hence need to take a view whether or not their company is complying with ITA 2008.

This news letter proposes to address the requirements of those CxOs who are keen to be empowered with updated information on Cyber Laws and how the laws affect Corporate Management in India. It will provide technical and legal inputs along with relevant news collated from other sources. We intend carrying articles, interviews and provide for interaction with the readers through Feedback and Questions and Answers sections.

The focus of the news letter will be the top management in the industry, both IT and non IT. However, legal practitioners may also find it useful. Readers may also find it useful to refer to the website www.naavi.org.

*This being an inaugural issue, more emphasis is placed on discussing the “Need for Cyber Law Knowledge for CxOs”. The **Knowledge +** section includes a discussion on “**Intermediaries**” and how Cyber Laws affect them. In the subsequent issues there will be broader and deeper coverage of different aspects of Cyber Law so that the news letter would become an essential **Tool of Empowerment of the CxO s for the Digital Era.***

January 22, 2010

Interview of the Month-1



Dinesh Pillai, CEO, Mahindra SSG, is a certified BS 7799 Lead Auditor and heads an organization which specializes in Information Security Management Services.

Having set up the Physical Security Consulting Practice in MSSG, and working since its inception, he recently took over as head of MSSG. A Post Graduate in Electronic Engineering, Mr Dinesh has extensive experience in IS audit and implementation.

Mr Dinesh Pillai shared his views on the relevance of legal compliance to CxOs, in an e-mail interview with Naavi.

Do you think Information Technology Act has relation to the functional responsibilities of a CxO?

As per IT Act 2008, the responsibility of misuse of the information system rests with CxO. The act explicitly mentions that IT and other infrastructure must be protected from misuse and it expects the CxO to take necessary measures to achieve this. Moreover, CxO must prove that they had exercised necessary due diligence to prevent any contravention.

So far in most of the organizations, information security was not assigned to any CxO as a key responsibility and with this amendment in the IT act, CxO has no option but to tag the responsibility in clear terms to personnel or set of personnel and maintain demonstrable evidence to show that controls and procedures were implemented to prevent misuse.

This act does not leave any room for negligence on part of CxO.

How does ITA 2008 affect the certifications to be provided by a CEO under Clause 49 of SEBI listing regulations?

The CEO's certification under Clause 49 of SEBI is like a positive assurance report stating that his good offices have ensured that the financial statements, other statements and transactions are correct to the best of their knowledge present a true and fair view of the company's affairs and are in compliance with existing accounting standards, applicable laws and regulations.

This is CEO certification of the good governance framework to the board and we cannot ignore IT Governance and information Security in this.

It is only a matter of time when the certification of IT and information security governance will become a part of the clause 49 certification. This will involve areas like integrity, retention and availability of information. Some highly evolved organizations are making necessary modifications to the reporting framework to include these points.

Interview of the Month-1

What is the channel of information most suitable for CxOs to follow Cyber Laws that affect the Company?

Ideally the most suitable Information channels should be the websites and publications of Supreme Court, CERTIn, and Ministry of IT.

However, sometimes these sites are not updated. There is need of one single and updated government channel to avoid confusion .

While the IT act lays down the basic legal requirements, the operational part of the security procedures have been left with various agencies (prominently CERTIn).

This creates a lot of confusion in the minds of CxOs to have a reference point for cyber laws. Various rules which have been suggested in IT Act 2000 for Security have also been removed in the IT amendment (2008) Act. The best available way is go for the ISO 27001 Security certification and have a trusted partner help maintain it.



Dinesh Pillai, CEO, MSSG

How can Information Security practitioners incorporate Legal Compliance under ITA 2008 into IS audits?

Although the standard for Information Security is ISO27001, when it comes to audits, ISO19011 is commonly referred to, which lays down the guidelines for auditing.

Using this guideline to audit a domain in ISO27001 which refers to Compliance, Information Security practitioners should prepare a Checklist mapping sections/subsections of IT Act to ISO 27001 and carry out audits accordingly. (E.g. Section 85 of IT act can be mapped to Clause A.6.1.1 of ISO 27001).

Similarly various control and clauses of standards may also be mapped to IT Act. Where any section cannot be mapped the new controls and/or process should be designed.

What are the steps you suggest for a company to comply with ITA 2008?

Establishing ISMS framework in the organization certainly helps and goes beyond the requirements of Compliance. Certification on Information Security/IT Governance would certainly help achieve a third party perspective and assurance of practices followed. Organization should otherwise conduct frequent checks and Self assessment exercises to get a positive assurance on a periodic basis. Audit on Information Security Practices at least once in a year by credited and certified auditors helps in the overall compliance.

Interview of the Month.-2



Rajat Mohanty,
CEO Paladion

Rajat Mohanty is co-founder and CEO of Paladion one of the prominent players in Information Security audit and implementation, in India. An alumnus of IIT and IIM Kolkata, he brings a deeply analytical mind to solve business problems. He has set up a successful business around Information Security at Paladion. As part of Paladion, Rajat has worked with leading financial services firms across Asia, assisting in development of security architecture and strategy. Rajat has over 15 years of experience in information risk management and technology operations

Do you think Information Technology Act has relation to the functional responsibilities of a CxO?

Information Technology Act, as amended in 2008, has several provisions that impacts how enterprises create, use, share and retain electronic data, including protection of private data. A failure to meet these requirements can result in significant penalties, liability and damage to the organization's reputation.

From a regulatory perspective, top management is responsible for promoting a self sustaining level of operations that minimizes impact to the business through breaches of laws. Top management therefore need to take into account the amended IT Act which has become effective recently.

In my view, Information Technology Act not just impacts the IT department but several other business functions in today's enterprise. To take few instances- It can impact various contractual relations created, explicitly or implicitly, over electronic format, or It can impact the services offered to end customer, which are electronic in nature like e-commerce, e-banking, e-auction and others, or It can also impact an organization for any wrongful use of information assets by its employees. As you can see, these relate to functional activities of departments such as finance, delivery channels and human resources apart from IT and audit departments.

How does the Act impact the information security activities within a corporate?

Information technology Act requires organizations to apply the principle of due diligence for protecting the sensitive electronic data. While it has not yet prescribed the nature of protection measures, it calls for establishing reasonable security practices in the organization.

It is usually difficult to quantify what level of security can be called as reasonable for an organization, but adopting global standards of security and business continuity, such as ISO 27001 and BS 25999 certainly will help. However organizations will need to carry out detailed risk analysis of sensitive customer/personal data stored & managed by them and apply greater protection which can be demonstrated as being at par with similar technology or practices adopted by similar organizations worldwide.

As mentioned earlier, some of the activities around logging, monitoring, data retention and encryption will need to be aligned with the provisions of the Act. Also the end user awareness training will need to incorporate sessions on IT Act awareness.



**Rajat Mohanty,
CEO, Paladion**

What are the steps you suggest for a company to comply with ITA 2008?

As a first step, it is imperative that management interpret the applicability of relevant provisions of the Act to their specific business functions and assess the level of compliance. A quick exercise to determine the gaps that exist in business processes and IT processes will not take more than 2-3 weeks in most organization.

Based on results of such gap assessment, top management thereafter can direct necessary resources for staying compliant with the Act and for building appropriate culture for compliance.

Specifically, some of the actions that will be required for compliance will revolve around-

- Identification of personally sensitive data within the enterprise that needs to be protected
- Setting up reasonable level of security based on size and complexity of each organization
- Use of encryption and electronic signature systems
- Personal data acquisition and retention strategies
- Logging and monitoring of access and usage of personal data
- Policies on acceptable usage of information assets
- Contractual liabilities established with customers and partners

How can Information Security practitioners incorporate Legal Compliance under ITA 2008 into IS audits?

Organizations that are ISO 27001 certified needs to demonstrate compliance to relevant regulatory requirements. In the Indian context, IT Act will definitely become relevant for consideration under ISO 27001 certification. Therefore, the periodic audits carried out for maintenance and improvement of ISMS under the standard, will need to incorporate checks from provisions of IT Act.

Some of the checks can be-

- ❖ Whether organizations periodically carry out identification and risk assessment of sensitive private data
- ❖ Whether data retention schemes are in place and in compliance with regulatory requirements
- ❖ Whether authentication schemes are in compliance with the Act specially for contractual arrangements
- ❖ Whether system exists for adequate monitoring and collection of data pertaining to cyber incidents and computer misuse
- ❖ Whether end users are appropriately informed about their responsibilities for protection of electronic data

Seeds of a Cyber World War emanate from China:

Two developments from China have raised lots of concern to Cyber Space watchers. Firstly, China introduced a special Domain Name registration system which is a prelude to banning all unregistered domain names from access in China. This could isolate the Chinese population from the global information network so that they would not be influenced by the democratic thoughts.

Simultaneously the fight between Google and Chinese Government has led to the threat of Google withdrawing from China. This is a symbolic fight of one US corporation which has the biggest footprint in the Internet to resist the Chinese authoritarianism spreading in the Internet.

At this point of time it is not clear where the fight is heading. It could see either one of the parties buckling down under pressure or rallying of democratic forces behind Google to challenge China in Cyber Space. Though US may not like to have a conventional war with China, it may like to see a shadow war being fought in Cyber Space by rallying around Google. Uncertain days are ahead of us and Indian Corporates would do well to recognize this “Cyber China-Country Risk “ and factor it in their corporate policies.

Tech Mahindra Buys Back Patent Rights from UPaid:

When Satyam Computers received a notice from UPaid in 2008 demanding a compensation of US \$ 1 billion on account of the failure of their Patent case in US attributed to a possible forgery of two signatures in a Patent support assignment form signed by Satyam employees, the Indian Corporate world realized the threat of huge vicarious liabilities due of non compliance of laws and lack of awareness of laws in employees.

Indian Industry gives a Thumbs Up to ITA 2008

A study conducted by Data Security Council of India (DSCI) and KPMG in association with CERT-IN, 86% of the 150 respondents expressed a view that that ITA 2008 will establish a strong data protection regime. 77% of the respondents also consider that it provides assurance to its International partners. "Employee Non Seriousness" was identified as the highest concern with 64% of respondents highlighting the same.

Source Code Theft Case on Chinese Government

A law suit by a Californian Company has named seven Computer makers including Sony, Lenovo, and Acer along with the Chinese Government accusing them of willingly joining a Chinese Government plan to spread a software known as Green Dam Youth Escort, throughout the country. The Company, Cyber Sitter has stated that its 3000 lines of source code have been pirated to create the said software. Each of the computer makers complied with a Chinese government requirement to install Green Dam on new computers, or to include a CD containing the program with each new computer. The lawsuit claims that the computer makers eventually found out that the software included pirated code, but continued to comply with the government directive.

UK Domain Name Agency Blocks 1219 Domains

Nominet, the body responsible for the .uk internet addresses disconnected over 1,219 websites without any orders from a court based only on police assertions about criminal activity on the sites.

Many website owners were surprised that Nominet was prepared to disconnect so many sites on the evidence of police claims alone. Nominet maintained that it acted because there had been a breach of the contract agreed by the people behind the websites by providing false particulars about the owners of the domain names.

Internet is a Legal Right of the Citizens

Finland has passed a law making Internet, a legal right of the Citizens. What is interesting to note is that more than 95% in Finland already have Internet connectivity. Their present law requires that internet operate at a minimum of 1mbps with a caveat that it increase to 100mbps in next 5 years. France has already declared internet a human right. Finland is the first country in the world to establish Internet as a legal right.

HIPAA Suit filed on Health Net Inc

Health Net a health insurance company lost a laptop containing medical records of up to 1.5 million in unencrypted form. The Company reported the lost records in November 2009 after 6 months of internal investigation.

Now a suit has been filed by Connecticut state attorney, both for security breach as well as not notifying the affected customers. The complaint also seeks a court order blocking Health Net from continued violations of HIPAA (Health Insurance Portability and Accountability Act) by requiring that any protected health information contained on a portable electronic device be encrypted.

This case marks the first action by a state attorney general involving violations of HIPAA since the Health Information Technology for Economic and Clinical Health Act (HITECH) authorized state attorneys general to enforce HIPAA.

[Collected from various sources]

The Compliance Dilemma of an Intermediary

We have seen many cases under various provisions of ITA 2000/8 where Cyber Café owners in India have been pulled up for the misuse of the facilities by their customers. We might have then wondered how the innocent Cyber Café owner can be hauled up for the offence committed by a user of his facility.

In 2004, Indian Corporate world was struck by the realization that even a Corporate CEO can face the same fate as the Cyber Café owner, when a member of baazee.com service uploaded an illegal content to the e-auction site and the CEO of baazee.com was charged with an offence under Section 67 of ITA 2000 which technically exposed the CEO to the risk of imprisonment up to 5 years.

This incident drew the attention of the corporate world for the first time to the vicarious liabilities provisions of ITA 2000 (Information Technology Act 2000) applicable to “Intermediaries”. ITA 2008 (ITA 2000 as amended by Information Technology Amendment Act 2008) has further enhanced the responsibilities of “Intermediaries” and Companies need to take due notice that their responsibilities have also increased correspondingly. In other words, CEOs need to examine under what circumstances, they fit into the definition of “Intermediaries” and face the vicarious liabilities as provided in the Act.

According to Sec 2(w) of ITA 2008,

"Intermediary" with respect to any particular electronic records, means, any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.-

This definition includes any organization which handles information on behalf of another person. This means that “Ownership of information handled” is a key issue to determine if an organization is an “Intermediary” or not. By handling information not belonging to oneself, the organization would be exposed to the possibility that such information could be instrumental in contravening any of the provisions of ITA 2008.

Normally, a Company owns all the information generated by itself. However, occasionally, it also handles information that belongs to its clients, as in the case of BPOs or Internet service providers or Mobile service providers or Telecom companies. Companies also handle information belonging to its employees. In such cases, it assumes a role of an “Intermediary”.

At a time when “Cloud Computing” is becoming the order of the day and “Outsourcing” is already established as a model of business, more and more companies offer services to third parties and all of them are open to the risks arising out of handling third party information. Hence the relevance of the definition of “Intermediaries” is felt by many companies.

...Contd

There are many offences under ITA 2008 that may be committed with the use of data or information in electronic form. It could be connected with obscenity as in the case of baazee.com or with false information hosted on a web page. There could be Phishing, Cyber Stalking, Advance Fee frauds and of course theft of identity information such as Credit Card data. There could be e-mails and SMS messages which may carry terrorist messages. There could be malicious codes bundled with other content and delivered to unsuspecting victims.

Any of these kinds of poisonous information handled by a system owned by the Company could be considered as an “Offence Committed by the Company”. Though the offence is actually committed by a third party, the Company and its officials would have to bear the vicarious liability under Section 85 of ITA 2008 unless they can establish that they have practiced “Due Diligence”.

There is also Section 79 of ITA 2008 which is important to determine if an “Intermediary” is liable for the offences committed with the use of information which it handles in its capacity as an “Intermediary” but does not belong to itself.

During the time the amendments to ITA 2000 were being considered, there was a good debate on the need to provide a safety net for “Intermediaries” such as baazee.com being held liable for the offences committed by the users of their services. Even in ITA 2000, the section 79 provided the escape clause for Intermediaries stating that “An intermediary shall not be liable...” if certain conditions are fulfilled. This section has been slightly modified in ITA 2008 and the section now reads as under.

Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not-

- *(i) initiate the transmission,*
- *(ii) select the receiver of the transmission, and*
- *(iii) select or modify the information contained in the transmission*

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf

...Contd

(3) The provisions of sub-section (1) shall not apply if-

- *(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act*
- *(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner*

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary

Essential aspects of Section 79 which we may note are,

- a) When an intermediary receives knowledge that some unlawful act is being committed with information under his control, he needs to “expeditiously” remove or “disable access”, “without vitiating the evidence in any manner”.
- b) The intermediary shall observe “Due Diligence”.

Thus both under Section 85 and Section 79, it becomes essential for the Intermediary to establish that it is practicing “Due Diligence”.

Unfortunately, the term “Due Diligence” cannot be easily reduced into a “Check List”. Though ITA 2008 was notified to be effective from October 27, 2009 and all sections including Section 79 of ITA 2008 have become effective from October 27, 2009, Rules under Section 79 have not yet been notified.

Similarly, one more section which has become effective against the Intermediaries but for which the rules are not yet notified is Section 67C which talks about preservation and retention of information. This section states

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

This section when read with Section 79 indicates that information which may form an “Evidence” and any other information that may be specified by the Government at some point of time in future when the rules under Section 67C is notified, need to be retained in an appropriate form for an appropriate time.

This is one of the many compliance obligations that Companies need to follow and document immediately. CxOs need to check if the requirement has been taken care of in their respective organizations. In order to understand all the implications of ITA 2008, it is necessary for the CxO to conduct an ITA 2008 compliance audit and take necessary steps for compliance.

Naavi

Questions and Answers

We intend using this section of the news letter to answer the Cyber Law related queries raised by our readers. This being an inaugural issue, we don't have any questions to be answered.

We hope that this would be one of the most vibrant sections of this news letter which may generate illuminating debates which would be of use to one and all.

We appreciate if queries are raised by persons indicating their Name, Occupation and Contact details. We however don't want to restrain the readers from raising questions without revealing their identity. Such readers may therefore send the questions as "Anonymous" in which case even their e-mail ID would not be provided on the news letter.

All questions may however be sent by e-mail to naavi@in.com by e-mail with the subject line containing "Cyber Laws for CxOs".

Since there are no questions from the readers in this inaugural issue, we will raise a question for all the readers and invite answers.

"Cyber Laws have been in force in India since October 17, 2000 and some of the provisions of the law required compliance by Companies. However many companies ignored ITA 2000 compliance as a part of their management focus. Some of them even declared under Corporate Governance Certification (under clause 49 of SEBI regulations) that they were complying with all regulatory requirements.

What according to you were the three principle reasons for the Companies to ignore ITA 2000 and what are your suggestions to correct the prevalence of a non compliance environment?

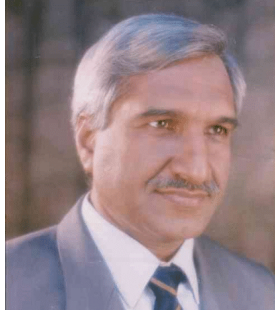
Editor



**Naavi's ITA 2008 Emergency Help Center
for Corporate Directors and CEOs**

Call Now or E-Mail: 91-9343554943 : naavi@vsnl.com

Messages



M.Rakesh Goyal
www.sysman.in

The e-newsletter on Cyber Laws for CxO is the most appropriate initiative taken by Naavi. It is the need of the hour. With Information Technology Act-2008 notified, CxO has lot of responsibilities and compliance requirements. In the current scenario, there is a big gap between the knowledge required and knowledge available regarding IT related laws and legal provisions, both national and international. This newsletter will fill this gap effectively.

I congratulate Naavi for this timely initiative. Naavi is one of the best suited persons to edit and publish this newsletter, given his expertise, experience and exposure to the provisions of IT Act, since year 2000.

I am sure that this newsletter will be most useful and appreciated by the CxO fraternity and also other users including researchers, policymakers, law enforcement, judiciary, advocates and IT Security students.



Ravi
Jagannathan

I congratulate Naavi on the initiative to launch a news letter for CxOs to provide Cyber Law related information to the business managers.

This was a long felt need of the industry since adoption of ITA 2000 requirements in the industry has been very slow. Partly this delayed response was due to the lack of adequate information flow to the CxOs.

I suppose this news letter would fill this information gap and catalyse the industry to adopt Compliance requirements as envisaged under the Indian laws.



V.Rakesh Nag
IIMA-Student

During a project assignment at IIMA in the first year, I worked on the subject of Information Security and realized its dependence on Cyber Laws- a subject that CXO's are coming to terms with only recently.

I therefore decided to join the online course in Cyber Laws at Cyber Law College so that by the time I graduate and join the industry, I will have acquired some of the skills to manage the legal aspects of Information Security, which I believe will be critical going ahead.

Recently, I also came to know that another management institute in Ghaziabad has introduced a regular course in Cyber Law. This has set the trend and I expect that Information Security management will become an integral part of Management education in India in the near future.

I will soon enter the industry where I will be required to manage businesses totally dependent on Information. I believe this news letter would be of immense help in keeping me up to date with developments in the field of Cyber Law which will be critical as I work my way towards being a CxO in the future after passing out from IIMA.

Naavi has received a few personal messages from friends with official responsibilities who have appreciated the introduction of this news letter but have expressed their desire not to be quoted for their own reasons. We respect their sentiments and express our appreciation for their support. *...Naavi*

Disclosure

This is an e-news letter published by Ujvala Consultants Pvt Ltd, No 37, “Ujvala” 20th Main, B S K Stage I, Bangalore 560050. (Ph: 080 26603490). Web: www.ujvala.com. E Mail: ujvala@md2.vsnl.net.in

The news letter is being edited by Naavi, Na.Vijayashankar, no 37/5, “Ujvala”, 20th Main, B S K Stage I, Bangalore 560050. Web: www.naavi.org. E Mail: naavi@in.com

A copy of the news letter is also being hosted on the website <http://www.cyberlaws4cxo.com>. In future the news letter may be reproduced in any other website owned by the same management or its assignees.

The views expressed in the news letter and the hosting website would be considered as belonging to the respective authors and provided for educative purpose and are not considered as legal advise.

Any comments and complaints if any may be sent to the editor at naavi@in.com for resolution.

Contents of this news letter may be reproduced only on specific permission from the editor and with due credit.

Copyright in respect of any contributions from authors published in the news letter will be deemed to have been transferred to the publisher at the time the article is submitted for publication. In the event an author intends to publish the same article in any other publication, he shall inform the publisher of Cyber Laws For CxO the name of such other publication and also add a note “First submitted for publication with Cyber Laws For CxO” in the other publication.

Any dispute arising out of the publication shall be settled through arbitration through the virtual arbitration center <http://www.arbitration.in> as per the terms of the Indian Arbitration and Conciliation Act 1996.