



Amendment in the Information Technology Act, 2000- An introduction

The traditional legal system has not been able to keep pace with the technological advancement in the information technology sector. The changes in the information technology by way of introduction of new hardware and software systems happens rapidly and the legislative enactments as well as amendments to the same are always slow to respond to such changes. The reason for this can be attributed to the fact that the law making process as well as the amendments to the law is a slow and tedious process which is made to respond to the old system in which circumstances triggering change in law would not change so often.

The Parliament has recently amended the Information Technology Act, 2000 ("Act") by way of the Information Technology (Amendment) Act, 2008 ("Amendment Act"). There are wide spread amendments in the Act which seem to be prompted by the recent changes in the IT Sector viz proliferation of internet, MMS clippings, auction sites and service provider liability issues.

This article attempts to elaborate on the changes in the Act relating to data privacy provisions and allowing compounding of certain offences.

Introduction of data privacy provisions:

Section 43 A has been inserted after section 43 of the Act, which provides that where a body corporate possessing, dealing or handling any sensitive personal data and information in a computer resource which it owns, controls or operates is negligent in implementing and maintaining reasonable security practises and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.



An analysis of Section 43-A shows that an obligation has been cast on a body corporate to maintain reasonable security practises and procedures in relation to data security. In the event such body corporate is not able to maintain the reasonable security practices and procedures, as a result of which wrongful loss or wrongful gain is caused to any person, such body corporate would liable to pay damages by way of compensation to the person so affected. Through the introduction of this Section an attempt has been made to bring data privacy in the domain of the Act, which is a step in the right direction. Though, in the explanation to the Section 43 A the term 'reasonable security practices and procedures' has been defined as to what has been specified between in an agreement between the parties or in any law for the time being in force and in the absence of any agreement or any law such reasonable security practises and procedures as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. In the experience of this author it is very difficult to lay down in the Agreement as to what reasonable security practises and procedures the parties are supposed to observe. In the absence of law defining reasonable security practises and procedures, the onus lies on the Central Government to come out with a code of reasonable security practises and procedures. Such code should not only lay down exhaustively the standard security practises and procedures but should be flexible enough to respond to the technological advancement in the IT Sector. In other words, such code should be amended from time to time to respond and to keep in pace with the latest technology advancements.

[Penalty and compensation for damage to computer, computer system etc:](#)

Section 43 of the Act has been amended by substituting in the marginal head, the word "penalty" with the words "penalty and compensation". The said substitution seems to be prompted by the fact that as per Section 73 of the Indian Contract Act, 1872 as well law settled through various judicial pronouncements, the compensation in the form of penalties is not allowed.

In Clause (a) of Section 43 after the words "computer network" the words "or computer resource" has been inserted. As per the Wikipedia, 'a computer resource is any physical or virtual component of limited availability within a computer system. Every device connected to a computer system is a resource. Every internal system component is a resource. Virtual system resources include files, network connections and memory areas'. This Clause sought to punish computer hacking and the introduction of the computer resource in the said Clause has enhanced the scope of coverage by bringing the unauthorised access to computer resources within the ambit of computer hacking.

The following two clauses have been introduced in Section 43 making the same punishable under the Act.

"(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) Steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter computer source code used for a computer resource with an intention to cause damage."

It is noteworthy that any destruction of information in a computer resource or diminishing its value or utility has been brought within the purview of the Act. Similarly, any theft or destruction of computer source code with an intention to cause damage has been brought within the purview of the Act so that the person causing it would be liable to pay damages by way of compensation.

Section 43 has been amended by removing the cap of Rs.1 Crore on damages by way of compensation to the affected person. Thus, the affected person can demand damages exceeding an amount of Rs.1 Crore.

Compounding of certain offences:

Section 77 A has been introduced which provides that a court of competent jurisdiction may compound offenses, which attracts imprisonments for a term less than three years. In such case, the accused may file an application for compounding in the court in which offence is pending for trial and the relevant provisions of the Cr.P.C. in relation to compounding shall apply to compounding of offence committed under the Act. There are three exceptions to such compounding. The first is where the accused by reason of his previous conviction is liable to either enhanced punishment or to a punishment of different kind. The second exception is where the offence affects the socio economic conditions of the country and the third exception is where the offence has been committed against a child below the age of 18 years or a woman. While the other two exceptions are very clear, we will have to wait for judicial precedent to understand as to which are the offences which affect the socio economic conditions of the country and hence non compoundable.

Conclusion:

Though through the amendments cited above the provisions in respect of data privacy has been introduced, compounding of certain offences has been allowed and the scope of offences which are subject to damages by way of compensation has been widened, this author feels that data privacy laws needs more strength under the Indian laws. It is needless to emphasize that privacy of data and its protection is prime concern of the foreign investors who invest in the technology sector.

For further information on any subject raised in this article, please contact:



Rohit Jaiswal
Partner,
E rohit@singhania.in

This article published solely for the interests of clients and associations of Singhania & Partners. This document is for general guidance only and does not constitute definitive advice. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought.

Copyright © 2010 Singhania & Partners.