

Information Technology Act & Data Protection

Vakul Sharma

© Vakul Sharma. All Rights Reserved, 2010

When the Information Technology Act, 2000 was introduced – it was the first technology legislation introduced in India!

And when the Information Technology (Amendment) Act, 2008 came into existence* – it is to be seen as a *GameChanger!*

* *Effective from October 27, 2009*

What the Information Technology (Amendment) Act, 2008
promises to do?

It will bring a *paradigm shift* in data protection and privacy regime in India:

- Establishing a self regulation framework
- Maintenance of reasonable security practices and procedures
- Articulating “sensitive personal data or information”
- Adjudication related to data protection and privacy [civil liabilities]
- Providing criminal prosecution vis-à-vis data protection and privacy

Banks' & The Information Technology Act

- Banks providing Internet Banking and other support services can be classified as “*intermediaries*”

Defined as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record.....[section 2(1)(w)]

Banks' as Intermediaries

- Section 43A: Compensation for failure to protect data.
- Section 67C: Preservation and retention of information by intermediaries.
- Section 69B to comply with the directions to monitor and collect traffic data or information through any computer resource for cyber security.

- Section 70B to comply with the direction of the Indian Computer Emergency Response Team (CERT-IN) in the area of cyber security.
- Section 72A disclosure of information in breach of lawful contract.
- Section 85 offences committed by companies.

Sections

Penalties

43A	Body corporate liable to pay damages by way of compensation to the person so affected.
67 C	Imprisonment for a term, which may extend to 3 years and shall also be liable to fine.

Sections

Penalties

69B	Imprisonment for a term, which may extend to 3 years and shall also be liable to fine.
70B	Imprisonment for a term, which may extend to 1 year or with fine, which may extend to one lakh rupees, or with both.

Sections

Penalties

72A	Imprisonment for a term, which may extend to 3 years or with fine, which may extend to five lakh rupees, or with both.
85	No express provision vis-à-vis penalties and compensation. However, the onus is on the company and its Directors, Secretary and Officers to prove their innocence.

Banks' & Due Diligence Framework

Section 43 A

- (a) Have you defined the various components of “sensitive personal data or information” vis-à-vis users/customers?
- (b) Do you have a security policy? Is it documented?

Section 67C

Do you have the
electronic record
preservation and
retention policy?

Section 69B

Have you adopted/established any procedure and safeguard for monitoring and collecting traffic data or information? Is it documented?

Section 70B

Do you have the
documented procedure
to comply with the
requests of CERT-IN
regarding cyber
security incidents?

Section 72A

(a) Do you have an adequate privacy policy?

(b) Whether you have provided *opt-in/opt-out* clause in your privacy policy?

Quo Vadis

Have you appointed
designated
officer/nodal
officer/computer-in-
charge to comply with
the directions of
competent
authority/agency
under various
provisions of the Act?

Quo Vadis

Whether details of such
designated
officer/nodal officer
readily available
online (at your
website)?

Yet to see any Indian banking
website mentioning that it is IT
Act compliant!

Yes, sites do mention that they have US Patriot Act
Certification!!

Banks and Data Protection

Illustrations

Illustration 1

RBI's Guidelines on *Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks*. These Guidelines came into effect from November 3, 2006.

When Banks' enter into such 'Off-shore outsourcing of Financial Services' agreements – whether banks' perform due diligence vis-à-vis data protection regime existing in the host country?

Illustration 2

- *Master Circular on Credit Card operations (as amended upto July1, 2009):*

Protection of customer rights

- Right to privacy
- customer confidentiality

Card issuing bank to maintain to maintain a Do Not Call Registry (DNCR) of customers as well as non-customers

- The bank would be held responsible if a DNCN is called by its DSAs/DMAAs or call centres

Liability under section 66A(c): any electronic mail or electronic mail message* for the purpose of causing annoyance or inconvenience.....punishable with imprisonment for a term, extend to 3 years and with fine

*message or information created or transmitted or received on a computer resource/communication device

- The bank should not engage telemarketers, DSAs/DMAAs, who do not have a valid registration certificate from DoT as telemarketers.

On July 31, 2008 the Hon'ble Supreme Court in the case of *Harsh Pathak vs. Union of India & Ors* passed directions in a PIL. It directed that any telemarketer who is not registered with Department of Telecommunication (DoT) should not be permitted to operate the telemarketing services.

The question is whether banks can be held liable -

(a) under section 66A(c) of the Information Technology Act, 2000, and

(a) for violating the Supreme Court Directions

Illustration 3

- Section 70 Protected system, wherein the appropriate Government is being empowered to declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure (CII)
- *Critical Information Infrastructure “.....means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety”

- It's time that RBI/IBA should initiate the process of including banking networks, data centres, INFINET, National Financial Switch (NFS) etc. as CII under section 70 of the Act.

Illustration 4

- In *Umashankar Sivasubramaniam case* decided by the Adjudicating Officer [Sh.P.W.C.Davidar] , Chennai*, it was held:

“The Respondent bank has failed to put in place a foolproof Internet Banking system with adequate levels of authentication and validation which would have prevented unauthorised access....found guilty of the offences made out under section 85 r/w section 43 of the Act”

* 12.04.2010

Data Protection under the Act

Civil liabilities under section 43, 43A	Criminal liabilities section 66, 66A, 66B, 66C, 66D, 67C,69B,70B, 72A and 85
---	--

Thanks

vakulsharma@gmail.com

© Vakul Sharma. All Rights Reserved, 2010