KHAITAN &CO

Advocates since 1911

Cross-Border Data Privacy and Security Best Practices

Supratim Chakraborty

| Mumbai | 13 February 2013

News Flash

- June 2012 - Website of a multinational internet corporation was reportedly hacked and more than 453,000 login credentials were stolen
- February 2012 - Website of an Indian subsidiary of a US software giant was reportedly hacked and login IDs and passwords of users were stolen
- May 2011 - Website of a major news channel was reportedly hacked and stolen personal details were published on a file sharing website
- April – June 2011 - Network of a major video game company was reportedly intruded and details from approximately 77 million accounts were stolen

…and the list goes on…

Celebrating a Century

Introduction

Changed Global Scenario

- Technology has made it possible to collect, copy, process and transfer data at the press of a button
- Risk and actual instances of misuse of data has increased, resulting in heightened attention from all global organizations for protection
- Data Privacy and protection has to be dealt by most companies from multiple jurisdiction standpoint, applying territorial laws

Celebrating a Century

The Law

Indian Legal Framework and Development

- Admittedly, there is no exclusive Data Protection legislation in India yet; although legal protection mechanisms exist
- Article 21 of the Constitution of India protects life and personal liberty which includes the Right to Privacy
- Information Technology Act ("**IT Act**") has made a beginning
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ("**Privacy Rules**") framed under Section 43A of the IT Act provides framework for protection of data
- A **Press Note** dated 24 August 2011 clarifies a number of provisions of the Privacy Rules
- Proposed Measures:
  - Right to Privacy Bill 2011
  - Nine National Privacy Principles set out by a panel working on new legal framework for India

Celebrating a Century

IT Act

Relevant Provisions

- Section 43 A – Civil Remedy:
  - Relates to any body corporate possessing, dealing or handling any **sensitive personal data or information** in a computer resource
  - Where such body corporate is negligent in implementing and maintaining **reasonable security practices and procedures**
  - Causes wrongful loss or wrongful gain to any person
  - Liable to pay **damages by way of compensation** to the affected person

- Section 72 A – Criminal Remedy:
  - Relates to any person providing **services under lawful contract** wherein personal information is accessed
  - There is intent or knowledge of wrongful loss or wrongful gain being caused through disclosure of such personal information
  - Disclosure is made **without the consent of the person** concerned **or in breach of a lawful contract**
  - Liable to be **punished with imprisonment** up to **3 years**, or with **fine** up to **INR 0.5 Million**, or with **both**

Celebrating a Century

Section 43-A and 72-A: Distinction

Particulars	Section 43-A	Section 72-A
Liability on	'Body corporate'	'Any person'
Information involved	'Sensitive personal data or information'	'Personal information'
Procurement of the information	Possessing, dealing or handling, in any manner	Procured whilst providing 'services under the terms of lawful contract'
Offence	Negligence in implementing and maintaining 'reasonable security practices and procedures' thereby causing wrongful loss or wrongful gain	Disclosure of personal information to another person without the consent of the person concerned or in breach of lawful contract
Mens Rea (criminal intention or knowledge)	Not Applicable	Element of mens rea should be present

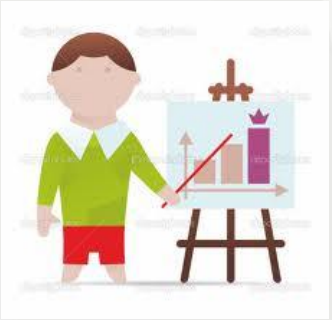
Celebrating a Century

Section 43-A and 72-A: Distinction

Particulars	Section 43 – A	Section 72 - A
Type of Information	Restricted to information in a computer resource	Information may be in any form, including physical documents
Penalty	Damages	Imprisonment for a term which may extend to 3 years or fine which may extend to INR 0.5 Million or both

Celebrating a Century

Explanation to Section 43-A of the IT Act



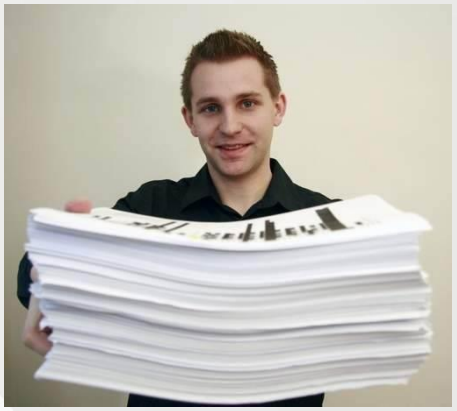
- **Body Corporate** - any company, including a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

- **Reasonable Security Practices and Procedures** - security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties **or** as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit ***(emphasis supplied)***

- **Sensitive Personal Data or Information** - such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit

Celebrating a Century

Privacy Rules



Key Definitions

- Sensitive Personal Data or Information ("**SPDI**") — personal information relating to:
  - password
  - financial information such as bank account or credit card or debit card or other payment instrument details
  - physical, physiological and mental health condition
  - sexual orientation
  - medical records and history
  - biometric information
  - any detail relating to the above as provided to body corporate for providing service
  - any information received under the above by body corporate for processing, stored or processed under lawful contract or otherwise

- The Rules also define **Personal Information** as:

  Information that relates to a **natural person**, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is **capable of identifying such person**

Celebrating a Century

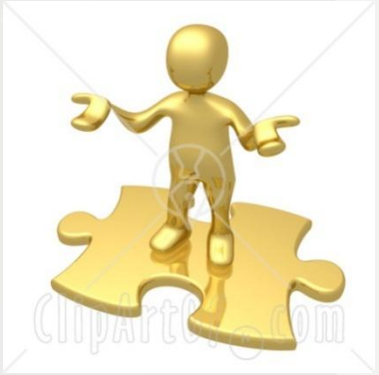
Privacy Rules – What To Do

Implementation of Reasonable Security Practices and Procedures

- As per agreement; or
- International Standards IS / ISO / IEC 27001 relating to 'Information Technology - Security Techniques - Information Security Management System - Requirements' ("**Standards**"); or
- Any code of best practices for data protection prepared by an industry association and approved and notified by the Central Government ("**Code**")
- Bodies corporate who have implemented such Standards or Codes require certification from Central Government approved auditors:
  - at least once a year; or
  - in case of significant upgradation of process and computer resource

Celebrating a Century

Privacy Rules – What To Do



Collection of Information

- SPDI to be collected only if necessary and required for lawful purpose
- Information to be used only for the purpose for which it is collected
- Information provider should know that:
  - information is being collected
  - the purpose of collection
  - the intended recipients
  - name and address of agency collecting and retaining the information
- SPDI not to be retained for longer period than required
- Information provider should be allowed to review / amend the information provided and the option to withdraw consent at any time
- In case of withdrawal of consent, the body corporate may not provide the goods or services for which the concerned information was sought

Celebrating a Century

Privacy Rules – What To Do

Disclosure of SPDI to Third Party

- As per agreement; or
- Obtain prior permission from the provider

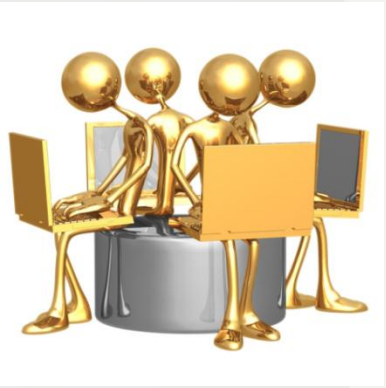
Consent for Purpose

- Obtain prior consent from provider of SPDI regarding purpose of usage

Transfer

- Permitted to transfer information to any person or body corporate located anywhere, who ensure the same / equal level of data protection; and
- Only if the transfer is necessary for the performance of lawful contract between the body corporate and provider of information or where such provider of information has consented to the transfer

Privacy Rules – What To Do



Privacy Policy

- Provide a Privacy Policy to information providers and publish the same on website
- Privacy Policy shall contain:
  - type of information collected
  - purpose for collection of information
  - security practices and procedures followed
  - disclosure policy

Grievance Officer

- Designate a Grievance Officer to address grievances of information providers
- Name and contact details of Grievance Officer to be published on website
- Grievance Officer to redress the grievances within one month

Celebrating a Century

Best Practices

Follow the 5 P's

Provider's agreement

Privacy policy

Procedures for information security

Pro-active monitoring

Purge the unnecessary

Celebrating a Century

Copyright and Disclaimer

- All rights, including copyright, in the content of this presentation are owned or controlled by Khaitan & Co and are for the reader's personal non-commercial use

- Except where expressly stated no person shall, without the prior express written permission of Khaitan & Co, copy, transmit, share with a third person, adapt or change for any purpose whatsoever the content of this presentation

- The contents of this presentation are for informational purposes only and are intended, but not guaranteed, to be correct, or complete, or up to date and Khaitan & Co disclaims all liability to any person for loss or damage caused by errors or omissions, whether such errors or omissions arise from negligence, accident or any other cause

- Khaitan & Co accepts and undertakes no liability for the interpretation and/or use of the information contained in this presentation, nor does it offer any warranty in respect of the contents hereto, of any kind, whether expressed or implied

Celebrating a Century

THANK YOU

www.khaitanco.com