



KHAITAN
& CO

Advocates since 1911

Data Privacy and Data Protection Key Legal Issues

Supratim Chakraborty | Ritwik Kulkarni

Mumbai | 14 January 2015

Bengalure

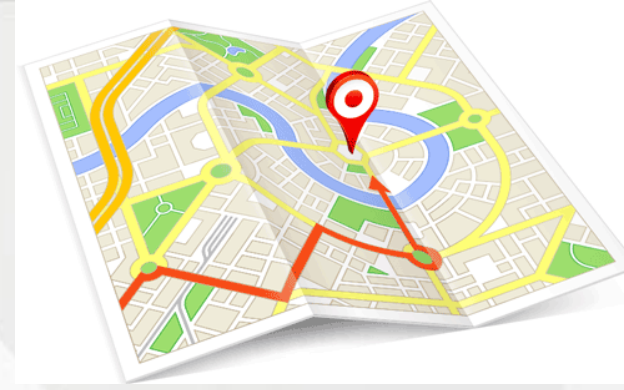
Kolkata

Mumbai

New Delhi



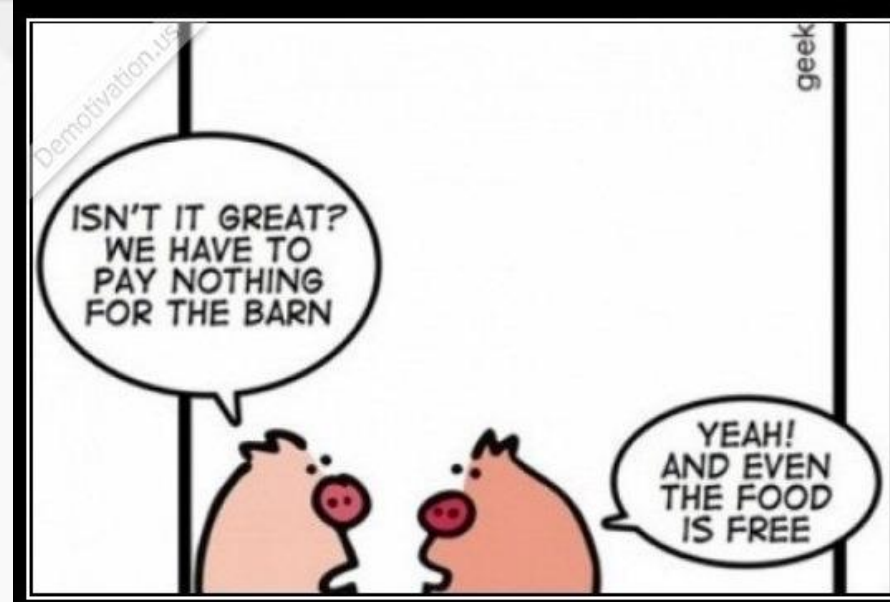
Route Map of the Presentation



- Why Data Privacy/Protection?
- Whom have we assisted – a snapshot
- Present Legal Framework
- Why is this important for most legal practice areas
- Case Studies
- Best Practices | In a Nutshell
- Q&A



Why Data Privacy / Protection?



- Global data flows
- Cloud Computing
- Economic Importance of data processing
- “Free” Internet Services
- E-commerce requires collection customer data
- “Big data” analyses and new markets



Whom have we Assisted – a Snapshot

TOSHIBA

Leading Innovation >>>

JPMORGAN CHASE & CO.



SIEMENS

- Whom have we assisted – a snapshot

iGLOBAL LAWTM
GLOBAL LABOUR LAW



Kodak alaris

NAVER



VISA STEEL



Whom have we Assisted – a Snapshot



GROUPON

facebook



UNITEDHEALTH GROUP*



SAMSUNG

WALT DISNEY

SYNOPSIS®
Accelerating Innovation

NOKIA





Present Legal Framework



- No exclusive Data Privacy / Data Protection legislation
- Article 21 of the Constitution protects life and personal liberty which includes the Right to Privacy
- Information Technology Act (“**IT Act**”)
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (“**Privacy Rules**”)
- A **Press Note** dated 24 August 2011



IT Act | Relevant Sections



- 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



IT Act | Relevant Sections



- 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**



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

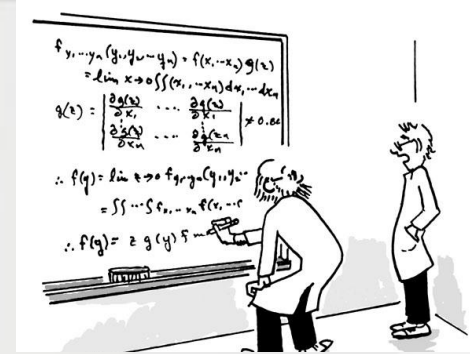


Section 43-A and 72-A: Distinction

Particulars	Section 43 – A	Section 72 - A
Mens Rea (criminal intention or knowledge)	Not Applicable	Element of mens rea should be present
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



Explanation to Section 43-A



- **Body Corporate** - company, 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
- **Sensitive Personal Data or Information** - such personal information as may be prescribed by the Central Government...



Privacy Rules



- 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...



Privacy Rules



- 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**



Case Law: Amit Patwardhan Vs BoB

[Secretary (information Technology), Govt. of Maharashtra]



- Bank Account Statements held to be SPDI
- Amit Patwardhan not awarded any amount in the first case with his employer
- In the present case, Bank of Baroda asked to pay a token compensation of Rs 5,000



Reasonable Security Practices / 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



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



Collection of 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





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





Privacy Rules – What To Do



www.shutterstock.com · 157778648

Privacy Policy

- Provide a Privacy Policy to information providers and publish 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
- Name / contact details of Grievance Officer to be published on website
- Grievance Officer to redress the grievances within one month



Importance for Most Practice Areas

Transaction Structuring

Due Diligence

Review of website T&Cs (e-commerce matters, etc)

Forensic Investigation Assistance (reporting)

Litigation and ADRs (data breach cases)

Employment / Labour Matters

Compliance and Training

Advisory

Others





Transaction Structuring / Issues

- Assess the sector carefully and structure
- Whether data room contains SPDI?
- Can we ring fence?
- Adequate Representations and Warranties
- Indemnities (specific indemnities, if required)
- Any employee / vendor / supplier consents?





Due Diligence – Basic Queries



- Is company collecting any SPDI from anyone (e.g. employees, clients, customers, etc)
- Reasonable security practices and procedures adopted
- Audit details of reasonable security practices and procedures
- Copy of the privacy policy (along with web link)
- Sample consent letters (or email templates, etc) that is used
- Process of destroying the SPDI collected post the period of its intended use
- Details of the Grievance Officer (including relevant web link)



Website T&Cs – Intermediaries Issues



- Definition: *‘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.”*
- Privacy Rules apply to Intermediaries
- Information Technology (Intermediaries Guidelines) Rules, 2011 also apply



Case Study 1 | Cartelization



- India Co's German parent company received cartelization allegation through its electronic whistleblowing mechanism
- Employees of the India Co were allegedly involved in a cartel and their office equipment were sought to be scanned without their consent
- Employer's Code of Conduct / Email / Internet Usage policies reviewed
- Mechanism devised to review the data within India Co, ring fence SPDI, copy and transfer relevant information to Germany



Case Study 2 | Insurance Fraud



- Insurance company's customers received calls from people claiming to be from IRDA
- Callers had all details of customers, including SPDI
- Customers urged to change insurance companies
- Police / IRDA / other regulators approached
- KCO analyzed and advised on various aspects of this matter:
 - Criminal Law aspects
 - Breach of Data Privacy / Data Protection Laws
 - Breach of Insurance Laws
 - Liabilities under Consumer Protection Law
 - Others



Best Practices | In a Nutshell

Follow the 5 P's

Provider's agreement

Privacy policy

Procedures for information security

Pro-active monitoring

Purge the unnecessary







THANK
YOU

www.khaitanco.com