

# Internet Law

## Regulating Cyberspace and Emerging Technologies



**Rodney D. Ryder | Nikhil Naren**

Foreword by

**Shri Dipak Misra**

*Former Chief Justice of India*

### **Highlights**

- The Personal Data Protection Bill 2019
  - Digital brand management
  - Law relating to emerging technologies
  - Drafting of privacy policy
- AND Sample questionnaire to conduct IT audit in an organization.

B L O O M S B U R Y

Bloomsbury Professional India

# **Internet Law**

Regulating Cyberspace  
and Emerging Technologies

**Rodney D. Ryder**  
**Nikhil Naren**

**B L O O M S B U R Y**  
NEW DELHI • LONDON • OXFORD • NEW YORK • SYDNEY

First published in India 2020

© 2020, Authors

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage or retrieval system, without prior permission in writing from the publishers.

No responsibility for loss caused to any individual or organization acting on or refraining from action as a result of the material in this publication can be accepted by Bloomsbury or the authors.

The content of this book is the sole expression and opinion of its authors, and not of the publisher. The publisher and authors in no manner are liable for any opinion or views expressed by the authors. While best efforts have been made in preparing this book, the publisher makes no representations or warranties of any kind and assumes no liabilities of any kind with respect to the accuracy or completeness of the content and specifically disclaims any implied warranties of merchantability or fitness of use for a particular purpose.

The publisher believes that the content of this book does not violate any existing copyright/intellectual property of others in any manner whatsoever. However, in case any source has not been duly attributed, the publisher may be notified in writing for necessary action.

BLOOMSBURY and the Diana logo are trademarks of Bloomsbury Publishing Plc

ISBN 978-93-89714-95-1

10 9 8 7 6 5 4 3 2 1

Bloomsbury Publishing India Pvt. Ltd  
DDA Complex, LSC Building No.4  
Second Floor, Pocket C-6 & 7, Vasant Kunj  
New Delhi 110070  
Phone: +91-11-40574957, 40574954  
www.bloomsbury.com  
CIN: U22130DL2012PTC232353

*To provide feedback, please mail at [professionalbooks@bloomsbury.com](mailto:professionalbooks@bloomsbury.com)*

Printed and bound in India by Rajkamal Electric Press, Kundli

To find out more about our authors and books visit [www.bloomsbury.co.in](http://www.bloomsbury.co.in)  
Here you will find extracts, author interviews, details of forthcoming events and the option to sign up for our newsletters.

To Rebecca, Mark and Gunjan

*Rodney D. Ryder*

To my late Grandparents, Mummy, Papa, Andrie Di  
and Digital India

*Nikhil Naren*

## Introduction to Metacept®

---

The book – *Internet Law: Regulating Cyberspace and Emerging Technologies* is quite one of its kind. Wondering Why? Well, to answer the question, you 'll need to visit [www.metacept.com](http://www.metacept.com).

Metacept® has been created with an objective of developing and sustaining a platform for a productive discussion on the ever-evolving issues in the domain of Information Technology [InfoTech] and Intellectual Property Rights [IPR] Laws. It aims at promoting a diversity of viewpoints, ideas, and ideologies in this domain.

The website has a designated tab for this book in the main menu bar titled – 'Internet Law-Book' in the menu bar. The same can be accessed on : <https://metacept.com/internet-law-book/>. The purpose is to enable the readers of the book to locate the references [Protected Document Files (pdf) and Hyperlinks] which are mentioned in the book and available in the public domain at a single place. For the convenience of the readers there is a bifurcation of the Chapters on the website under the 'Internet Law-Book' tab.

One may visit the links of the Chapters and find the resource materials therein for further reading and gaining more information on a particular subject matter. Readers can also drop in their suggestions, complaints and/or feedback on [editor@metacept.com](mailto:editor@metacept.com). Therefore, this makes the book, *Internet Law: Regulating Cyberspace and Emerging Technologies* dynamic in its nature.

**NOTE: The Publisher, Bloomsbury, has no affiliation with the website – [www.metacept.com](http://www.metacept.com)**

## About the authors

---



**Rodney D. Ryder**

Rodney D. Ryder is the Founding Partner of Scriboard [Advocates and Legal Consultants], New Delhi, a full-service commercial law firm with cutting edge specialization in technology, new media, and intellectual property laws. He is the author of *Guide to Cyber Laws: the Information Technology Act, 2000, E-Commerce, Data Protection and the Internet*, the first section-wise analysis of the Indian Information Technology Act, 2000.

Mr. Ryder has been nominated as a 'Leading Lawyer' in intellectual property, technology, communication, and media law by Asia Law, Who'sWhoLegal, Asia Legal 500, amongst other International publications. Mr. Ryder was listed as one of India's leading lawyers in the '40 under 45' study conducted by WhosWhoLegal, United Kingdom. He counsels a wide range of clients from start-ups to the Fortune 100 and represents them in litigation regarding technology law, data security, compliance with law enforcement and intellectual property strategy. He is on the Board and Advisor to leading companies. He is regularly interviewed and widely quoted by Indian and International media on technology, intellectual property and new media laws.

His second book, *Intellectual Property and the Internet* [published by LexisNexis] has been acknowledged to be an authoritative work on domain name disputes by the Hon'ble Supreme Court of India and has been quoted in the first and only judgement by the Hon'ble Supreme Court of India on domain names [*Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.*; (2004) 6 SCC 145]. He is an advisor to the National Internet Exchange of India [NIXI] and a member of the panel of independent and neutral arbitrators with NIXI.



### **Nikhil Naren**

Nikhil is presently a 'Trainee Advocate' at Scriboard [Advocates and Legal Consultants], New Delhi after he received a Pre-Placement Offer (PPO) in the 7<sup>th</sup> Semester of his law school. He is presently in the 10<sup>th</sup> Semester of his Law School and is enrolled in the B.A.LL.B Programme. He religiously follows the practice of – Dreaming- Hoping- Working and Achieving. Over the years, he has built special inclination and interest towards Information Technology Laws, Intellectual Property Laws, Competition Laws and Contract Law amongst other areas of law. He holds a Diploma in Cyber Laws from Government Law College, Mumbai and Asian School of Cyber Laws, Pune and a Certification in Intellectual Property Law and Competition Law from Federation of Indian Chambers of Commerce & Industry (FICCI), New Delhi. He is currently pursuing certificate course in Blockchain and Social Media Laws from Enhelion. Additionally, he has also framed the chapters and developed content for the Certificate Course on Artificial Intelligence and Law for Enhelion.

He has authored Research Papers and loves to write blogs on contemporary issues falling under his domain of interests. Apart from this, he has also been an active member and Head of his Law School's Photography Society- One 'Click' and has a good experience at Moot Courts and Mock-Trial competitions. He also mentors law students for Moots, Research, Internships and on any other issues approached for.

He is a focused person with a strong belief in honesty and hard work. His objective in life is to continuously improve himself and to try new things that challenge him. He is a firm believer of the fact that "learning never stops."

**Research Associates**

Aman Shankar, Apoorva Tyagi, Asit Gupta, Aviral Srivastava, Deepika Punia, Dhairya Thakkar, Parth Sharma, Priyanshi Rastogi, Rhea Khanna, Shubhangi Singh, Sudiksha Gupta and Vanshika Arora

*Special Thanks to  
Symbiosis Law School, NOIDA*



# Table of contents

---

<i>Acknowledgement</i> .....	<i>xi</i>
<i>Introduction to Metacept®</i> .....	<i>xiii</i>
<i>About Scriboard [Advocates and Legal Consultants]</i> .....	<i>xv</i>
<i>About the authors</i> .....	<i>xvii</i>
<i>About the Research Associates</i> .....	<i>xix</i>
<i>Foreword</i> .....	<i>xxiii</i>
<i>Preface</i> .....	<i>xxix</i>
<i>Contents at a glance</i> .....	<i>xxxi</i>
<i>Table of cases</i> .....	<i>xliv</i>
<b>Chapter 1 Information Technology Act, 2000</b>	
1.1 Introduction.....	1.2
1.1.1 National and international reasons behind enactment of the Act.....	1.3
1.1.2 Aims and objectives.....	1.4
1.1.3 Overview of the Act.....	1.5
1.2 Penalty, Compensation and Adjudication.....	1.6
1.2.1 Section 43: [penalty and compensation] for damage to computer, computer system, etc.....	1.6
1.2.2 Section 43A: Compensation for failure to protect data.....	1.8
1.2.3 Section 44: Penalty for failure to furnish information, return, etc.....	1.8
1.2.4 Section 45: Residuary penalty.....	1.8
1.2.5 Section 46: Power to adjudicate.....	1.8
1.2.6 Section 47: Factors to be taken into account by the adjudicating officer.....	1.9
1.3 Information Technology (Amendment) Act, 2008.....	1.10
1.4 The Information Technology (Amendment) Bill, 2018.....	1.11
1.5 Compliance under the Information Technology (Amendment) Act, 2008.....	1.12
1.5.1 Identity theft.....	1.19
1.6 Critique of the Information Technology Act, 2000 and Information Technology (Amendment) Act, 2008.....	1.22
1.6.1 Spamming.....	1.23
1.6.2 Phishing.....	1.23
1.6.3 Information protection in internet banking.....	1.24
1.6.4 Cyber war.....	1.24

Internet law: regulating cyberspace and emerging technologies

1.6.5	Intellectual property infringement	1.25
1.7	Suggestions for improvement in the Information Technology Act, 2000	1.26
1.8	Conclusion	1.29

**Chapter 2 Cyber crimes**

2.1	Introduction	2.2
2.2	Existing penal provisions for different cybercrimes under the IT Act, 2000	2.4
2.3	Hacking	2.7
2.4	Denial of service attack	2.8
2.5	Phishing	2.10
2.6	Cyber stalking	2.13
2.7	Software piracy	2.16
2.7.1	What is software piracy?	2.17
2.7.2	Consequences of software piracy	2.19
2.7.3	Types of software piracy	2.20
2.7.3.1	Counterfeiting	2.21
2.7.3.2	Soft lifting	2.21
2.7.3.3	Internet piracy	2.21
2.7.3.4	Hard-disk loading	2.21
2.7.3.5	Commercial use of non-commercial software	2.22
2.8	Cyber terrorism	2.22
2.8.1	What is cyber terrorism?	2.23
2.8.2	Forms and essentials of cyber terrorism	2.24
2.9	Tampering with computer source documents	2.26
2.9.1	What are computer source documents?	2.26
2.9.2	Essentials to establish liability	2.26
2.9.3	Notable case laws relating to tampering of CSDs	2.27
2.10	Standard operating procedure (SOP)	2.28
2.11	Identity theft	2.29
2.11.1	Meaning of identity theft	2.29
2.11.2	Essentials of the offence	2.30
2.11.2.1	Wrongful procurement of unique identification information of a person	2.31
2.11.2.2	Wrongful use of such information for one's profit or with the intention of causing harm to that person	2.31
2.12	Sending offensive messages through communication service, etc.	2.31
2.13	Computer related offences and the Indian Penal Code	2.34

2.13.1	The Ukraine power grid attack . . . . .	2.35
2.13.2	Tallinn Manual 2.0 on the international law applicable to cyber operations (comprehensive guide) . . . . .	2.36
2.14	Reporting of cyber crimes . . . . .	2.38
<b>Chapter 3 Electronic evidence</b>		
3.1	Introduction . . . . .	3.2
3.2	The United Nations Commission on International Trade Law (UNCITRAL) & Civil Evidence Act, 1968 (United Kingdom) . . . . .	3.3
3.3	Vires of section 65-B, Indian Evidence Act, 1872 . . . . .	3.5
3.4	Case laws on electronic evidence . . . . .	3.6
3.5	Digital evidence and electronic evidence . . . . .	3.9
3.6	Certificate under section 65-B, Indian Evidence Act, 1872 . . . . .	3.11
3.7	Admissibility of various electronic evidence . . . . .	3.11
3.7.1	Hard disk . . . . .	3.11
3.7.2	Call records . . . . .	3.12
3.7.3	Proof of contents of CD . . . . .	3.13
3.7.4	Presumptions . . . . .	3.14
3.7.5	Electronic evidence examiner . . . . .	3.14
<b>Chapter 4 Internet security</b>		
4.1	Introduction . . . . .	4.2
4.2	Malware . . . . .	4.4
4.2.1	Static analysis . . . . .	4.9
4.2.2	Dynamic analysis . . . . .	4.9
4.2.3	Hybrid analysis . . . . .	4.10
4.3	Anti-virus . . . . .	4.11
4.3.1	Signature based detection . . . . .	4.11
4.3.2	Heuristic / Behaviour based detection . . . . .	4.12
4.3.3	Specification based detection . . . . .	4.12
4.4	Firewalls . . . . .	4.13
4.4.1	Packet filtering firewalls . . . . .	4.15
4.4.2	Application level gateway . . . . .	4.15
4.4.3	Circuit level gateway . . . . .	4.16
4.5	Stateful inspection firewalls . . . . .	4.16
4.6	Online digital profiling . . . . .	4.18
4.7	Internet protocol address . . . . .	4.22
4.8	Email security . . . . .	4.26
4.9	Blogging and online security . . . . .	4.30
4.10	Conclusion . . . . .	4.30
4.10.1	The threat of malware . . . . .	4.31
4.10.2	The threat of hacking . . . . .	4.31

Internet law: regulating cyberspace and emerging technologies

4.10.3	The threat of spamming, phishing and other attacks over emails	4.32
4.10.4	Voice phishing/phone scams	4.32

**Chapter 5 Interception and monitoring of electronic communication in India**

5.1	Evolution of the law of interception and monitoring in india	5.2
5.2	Law on interception and monitoring of electronic communication	5.6
5.2.1	Section 69 of Information Technology Act, 2000	5.7
5.2.1.1	Sub-section (1)	5.7
5.2.1.2	Sub-section (2)	5.9
5.2.2	Section 69A of the Information Technology Act, 2000	5.13
5.2.2.1	Constitutional validity of section 69A	5.19
5.2.2.2	Blocking of websites under section 69A	5.19
5.2.3	Section 69B of the Information Technology Act, 2000	5.21
5.3	State surveillance and the right to privacy	5.24
5.3.1	Section 69: unconstitutional?	5.27
5.4	Section 70B of the Information Technology Act, 2000	5.28
5.5	Retention of information by intermediaries	5.33
5.6	Retention and allied privacy issues	5.38
5.7	Encryption technology	5.41

**Chapter 6 Privacy**

6.1	Introduction	6.2
6.2	Law of privacy	6.3
6.2.1	Facets of privacy	6.3
6.2.1.1	Bodily privacy	6.4
6.2.1.2	Privacy related to personal life	6.4
6.2.1.3	Informational privacy	6.5
6.2.1.4	Communication privacy	6.5
6.3	Origin	6.6
6.4	Right to privacy	6.8
6.4.1	Constitutional basis	6.9
6.4.2	Privacy and freedom of speech	6.10
6.4.3	Privacy of public figures	6.11
6.4.4	Privacy and Right to Information Act	6.11
6.4.5	Privacy and communication	6.12
6.5	Breach of confidentiality and privacy	6.13
6.5.1	Breach of confidence	6.13
6.5.2	Breach of privacy tort in Indian law	6.16
6.5.2.1	Trespass	6.16
6.5.2.2	Nuisance	6.17

Table of contents

6.5.3	Remedies in privacy actions . . . . .	6.17
6.5.3.1	Injunction . . . . .	6.17
6.5.3.2	Prior notification . . . . .	6.18
6.5.3.3	Damages. . . . .	6.18
6.6	Data Protection Bill . . . . .	6.19
6.6.1	Features . . . . .	6.19
6.6.2	Highlights . . . . .	6.20
6.6.3	Comparison between privacy law in India with other countries . . . . .	6.21
6.7	General Data Protection Regulation (GDPR). . . . .	6.22
6.7.1	Scope . . . . .	6.23
6.7.2	Principles . . . . .	6.24
6.7.3	Rights of data subject. . . . .	6.25
6.7.3.1	Right to be informed. . . . .	6.25
6.7.3.2	Right to access . . . . .	6.25
6.7.3.3	Right to rectification . . . . .	6.25
6.7.3.4	Right to erasure . . . . .	6.25
6.7.3.5	Right to restrict processing . . . . .	6.26
6.7.3.6	Right to data portability . . . . .	6.26
6.7.3.7	Right to object . . . . .	6.26
6.7.3.8	Right in relation to automated decision-making including profiling . . . . .	6.26
6.7.4	Remedies, liability and penalties . . . . .	6.26
6.8	Right to be forgotten . . . . .	6.27
<b>Chapter 7 Data Protection Regime in India</b>		
7.1	Introduction . . . . .	7.1
7.2	Purpose of the Personal Data Protection Bill, 2019 . . . . .	7.3
7.3	Personal data . . . . .	7.3
7.4	Sensitive personal data . . . . .	7.4
7.5	Compliance . . . . .	7.4
7.6	Data fiduciary and data principal . . . . .	7.4
7.6.1	Social media intermediaries (SMI) . . . . .	7.5
7.6.2	Role of data fiduciary . . . . .	7.5
7.6.2.1	Requirements . . . . .	7.6
7.6.2.2	Penalties prescribed in the Personal Data Protection Bill, 2019 . . . . .	7.8
7.7	Brief study of the Personal Data Protection Bill, 2019 . . . . .	7.8
7.7.1	Chapter II & III - Obligations of data fiduciary and grounds for processing of personal data without consent. . . . .	7.8

Internet law: regulating cyberspace and emerging technologies

7.7.2	Chapter IV – Personal data and sensitive personal data of children . . . . .	7.10
7.7.3	Chapter V - Data principal rights [rights of individuals whose personal data are processed] . . . . .	7.10
7.7.4	Chapter VII - Transfer of personal data outside india [norms for cross-border transfer of personal data] . . . . .	7.12
7.7.5	Chapter VIII– Exemptions. . . . .	7.12
7.7.6	Chapter X - Penalties and compensation [remedies for unauthorised and harmful processing] . . . . .	7.13
7.7.7	Chapter XIII – Offences [protect the autonomy of individuals in relation to their personal data]. . . . .	7.14
7.8	Data Protection Authority of India . . . . .	7.15
7.9	Differences between Personal Data Protection Bill, 2019 and EU’s General Data Protection Regulation . . . . .	7.16

**Chapter 8 Freedom of expression in cyber space**

8.1	Freedom of speech and expression and the Indian constitution . . . . .	8.2
8.2	Freedom of speech and expression on the internet . . . . .	8.3
8.2.1	Methods of controls . . . . .	8.6
8.2.1.1	Pre-censorship. . . . .	8.7
8.2.1.2	Criminalisation . . . . .	8.7
8.2.1.3	Controlling outlets . . . . .	8.8
8.3	Reasonable restrictions. . . . .	8.8
8.4	Cyber defamation – introduction . . . . .	8.12
8.5	Essential ingredients of defamation . . . . .	8.13
8.6	Publication . . . . .	8.14
8.6.1	How . . . . .	8.15
8.6.2	When . . . . .	8.15
8.6.2.1	Multiple publications rule – and limited period. . . . .	8.16
8.6.3	Where. . . . .	8.16
8.6.4	Who . . . . .	8.17
8.7	Is the intermediary a publisher or otherwise responsible?. . . . .	8.18
8.7.1	The publishing process in a digital world . . . . .	8.18
8.7.2	From transmitter to publisher . . . . .	8.19
8.7.3	Section 79 of Information Technology Act, 2000 . . . . .	8.21
8.8	Statutory provisions to online defamation . . . . .	8.22
8.8.1	Sections 499-502 of Indian Penal Code, 1860 . . . . .	8.22
8.8.2	Information Technology Act, 2000 . . . . .	8.23
8.9	Limitation period for defamatory actions. . . . .	8.23
8.10	Judicial interpretation . . . . .	8.24
8.11	Where to lodge a complaint? . . . . .	8.26

Table of contents

8.12	Jurisdiction in cyber space – introduction .....	8.28
8.13	Three pre-requisites of jurisdiction .....	8.30
	8.13.1 Prescriptive jurisdiction .....	8.30
	8.13.2 Adjudicative jurisdiction .....	8.31
	8.13.3 Enforcement jurisdiction .....	8.31
8.14	International law/ jurisdictional theories in jurisdiction to prescribe .....	8.33
	8.14.1 Territorial principle .....	8.33
	8.14.2 Nationality principle .....	8.34
	8.14.3 Protective principle .....	8.35
	8.14.4 Passive personality principle .....	8.36
	8.14.5 The effect doctrine .....	8.36
	8.14.6 Universality principle .....	8.37
8.15	Extraditable offences .....	8.38
	8.15.1 Cyber crimes – are they extraditable offences? .....	8.39
8.16	Tests to determine jurisdiction in internet law cases .....	8.41
	8.16.1 Pre-long arm statute period .....	8.41
	8.16.2 The long arm statutes .....	8.41
	8.16.3 The effects test .....	8.42
	8.16.4 General and specific personal jurisdiction .....	8.42
	8.16.4.1 Specific jurisdiction in cyberspace .....	8.43
	8.16.5 The minimum contacts test for internet transactions .....	8.44
8.17	Indian laws to determine personal jurisdiction .....	8.45
	8.17.1 Selection of forum by choice .....	8.45
	8.17.2 Jurisdiction under Different Statute .....	8.45
	8.17.2.1 Relevant provisions of Code of Civil Procedure, 1908 (CPC) .....	8.45
	8.17.2.2 Relevant provisions of the Code of Criminal Procedure, 1973 .....	8.46
	8.17.2.3 Relevant provisions related to copyrights and trademarks .....	8.46
	8.17.2.4 Relevant provisions of Information Technology Act, 2000 .....	8.47
<b>Chapter 9 E-governance</b>		
9.1	Introduction .....	9.1
	9.1.1 Government to citizen (G2C) .....	9.2
	9.1.2 Government to business (G2B) .....	9.2
	9.1.3 Government to government (G2G) .....	9.3
	9.1.4 Government to employee (G2E) .....	9.3

Internet law: regulating cyberspace and emerging technologies

9.2	Legal recognition of digital records and signatures	9.4
9.2.1	Incorporation by reference	9.4
9.2.2	Legal recognition of electronic records (section 4 of Information Technology Act, 2000)	9.5
9.2.3	Legal recognition of digital signatures (Section 5 of Information Technology Act, 2000)	9.6
9.3	Electronic signature	9.7
9.3.1	Symmetric cryptography	9.8
9.3.2	Asymmetric system	9.9
9.3.3	Section 5 of Information Technology Act, 2000	9.9
9.4	Use of electronic records and signatures in government and its agencies	9.10
9.5	Use of digital signature in government services	9.11
9.6	Retention of electronic records	9.11
9.6.1	Electronic record retention policy	9.12
9.7	Laws of various nations and method in india	9.12
9.8	Digi locker system	9.13
9.9	E-governance models	9.15
9.9.1	The critical flow model	9.16
9.9.2	The comparative analysis model	9.16
9.9.3	The e-advocacy/mobilisation and lobbying model	9.16
9.9.4	The interactive-service model	9.17
9.10	Publication of rules, regulations, etc., in electronic gazette	9.17
9.10.1	Brief description of gazette	9.17
9.10.2	Power to make rules by the central government in respect of electronic signature	9.19
9.11	National e-governance plan (NeGP)	9.20
9.11.1	Vision	9.20
9.11.2	Mission mode projects	9.20
9.11.3	NeGP implementation strategies	9.24
9.11.4	NeGP governance structure	9.25
9.12	Aadhaar case study	9.27

**Chapter 10 E-commerce**

10.1	Introduction	10.2
10.2	United Nations Commission on International Trade Law	10.2
10.3	Models of e-commerce	10.3
10.3.1	B2B model	10.3
10.3.2	B2C model	10.3
10.3.3	C2B model	10.4
10.3.4	C2C model	10.4



Table of contents

10.4 Electronic data interchange (EDI) .....10.4  
10.4.1 How does EDI work? .....10.4  
10.4.2 Standardisation of EDI.....10.5  
10.5 Digital signature and electronic signature .....10.6  
10.6 Technical concept behind digital signature .....10.7  
10.6.1 Symmetric cryptography ..... 10.8  
10.6.2 Asymmetric cryptography .....10.9  
10.6.3 Hash function .....10.9  
10.6.4 Public key cryptography .....10.10  
10.6.5 Public key infrastructure (PKI) process .....10.11  
10.6.6 Digital signature illustration .....10.12  
10.7 Legal aspect behind digital signature .....10.13  
10.7.1 Digital signatures – technology specific v  
technologically neutral .....10.14  
10.7.2 Transition from digital signature to electronic signature..10.15  
10.7.3 Electronic signature .....10.16  
10.8 Liability of an intermediary in e-commerce .....10.18  
10.8.1 Liability in India .....10.19  
10.8.1.1 Avnish Bajaj v State of N.C.T Delhi .....10.20  
10.8.1.2 Amendment, 2008.....10.21  
10.9 Electronic contracts .....10.26  
10.9.1 Essentials of e-contracts.....10.27  
10.9.2 Relevant IT Act provisions .....10.28  
10.9.3 Types of e-contracts .....10.31  
10.9.3.1 Browse wrap .....10.31  
10.9.3.2 Shrink wrap .....10.31  
10.9.3.3 Click wrap .....10.32

**Chapter 11 Social media**

11.1 Introduction .....11.2  
11.2 Social engineering .....11.2  
11.2.1 Background .....11.2  
11.2.2 What is social engineering?.....11.3  
11.2.3 Reverse social engineering .....11.4  
11.2.4 Social engineering life cycle .....11.4  
11.2.5 Social engineering attack techniques.....11.5  
11.2.5.1 Phishing .....11.6  
11.2.5.2 Spear phishing.....11.6  
11.2.5.3 Baiting .....11.6  
11.2.5.4 Scareware .....11.6  
11.2.5.5 Water holing .....11.7  
11.2.5.6 Tailgating .....11.7

Internet law: regulating cyberspace and emerging technologies

11.2.6	Quid pro quo	11.7
11.2.6.1	Pretexting	11.7
11.2.7	Social engineering prevention and countermeasures	11.8
11.3	Fake accounts	11.8
11.3.1	Introduction	11.8
11.3.2	What is a fake account?	11.9
11.3.3	How to verify the authenticity of an account?	11.9
11.3.4	Is it illegal to create a fake account?	11.10
11.3.5	Can one report a fake account?	11.10
11.4	Popular crimes	11.11
11.4.1	Phishing	11.11
11.4.2	Social media conning	11.12
11.4.3	Identity spoofing	11.12
11.4.4	Hacking	11.12
11.4.5	Cyber bullying	11.12
11.4.6	Trade of illegal products	11.13
11.4.7	Robberies	11.13
11.4.8	Stalking	11.14
11.5	Precautionary steps	11.14
11.5.1	E-mail verification	11.14
11.5.2	Time and IP address-based restrictions	11.14
11.5.3	reCAPTCHA	11.15
11.5.4	Challenge questions and puzzles	11.15
11.5.5	Crowd reporting	11.15
11.6	Confidential information leak	11.15
11.6.1	Introduction	11.15
11.6.2	How is data leaked?	11.16
11.6.3	What are the consequences of data leakage?	11.17
11.6.3.1	Consequences related to consumers	11.17
11.6.3.2	Consequences related to the firm	11.17
11.6.3.3	Data leak prevention	11.18
11.6.4	Summary of existing DLPD techniques	11.20
11.6.5	Challenges in big data protection	11.20
11.7	A tool for spreading spam and malware	11.21
11.7.1	Phishing	11.21
11.7.2	Impersonation	11.21
11.7.3	Spying	11.22
11.7.4	Hacking	11.23
11.8	Terms of privacy	11.23
11.8.1	Electronic voyeurism	11.23
11.8.2	Data retention	11.24

11.9	Spam apps .....	11.24
11.10	Whatsapp's spyware attack.....	11.25
<b>Chapter 12 Intellectual property and information technology</b>		
12.1	Introduction .....	12.2
12.2	Copyright in Digital Medium.....	12.8
	12.2.1 Copyright in computer programs.....	12.9
	12.2.2 Existence of copyright .....	12.11
	12.2.3 Exclusive rights.....	12.18
12.3	Materials on the Internet .....	12.19
12.4	Copyright and International Treaties .....	12.20
12.5	John Doe Orders .....	12.21
12.6	Right to Fair Use.....	12.24
12.7	IPR and Memes .....	12.26
12.8	Trademarks, Domain Names and the Internet.....	12.27
12.9	Basics of Trademark.....	12.28
	12.9.1 Meaning of trademark .....	12.28
	12.9.2 Essentials of a trademark.....	12.28
12.10	Rights of Trademark Holder .....	12.29
12.11	Trademark Infringement and Remedies .....	12.31
	12.11.1 Infringement under Trade Marks Act, 1999.....	12.32
	12.11.2 Passing off .....	12.34
12.12	Trademark Infringement on the Internet .....	12.36
12.13	Domain Names and Domain Name Disputes .....	12.37
	12.13.1 Domain names .....	12.37
	12.13.2 Anatomy of a domain name .....	12.38
	12.13.2.1 Generic top-level domains (gTLDs).....	12.39
	12.13.2.2 Country code top-level domains (ccTLDs) .....	12.39
	12.13.2.3 Second-level domains (SLDs).....	12.39
	12.13.3 Registration of domain names .....	12.40
	12.13.4 Domain names as trademarks.....	12.41
	12.13.5 Domain name disputes .....	12.42
	12.13.6 Types of domain name disputes .....	12.43
	12.13.6.1 Cybersquatting .....	12.43
	12.13.6.2 Typosquatting .....	12.44
	12.13.6.3 Reverse domain name hijacking.....	12.44
	12.13.6.4 Palming off disputes .....	12.44
	12.13.6.5 Parody or protest website disputes.....	12.44
	12.13.7 Domain name protection.....	12.45
	12.13.7.1 Resolution of domain name disputes through traditional law.....	12.45

Internet law: regulating cyberspace and emerging technologies

12.13.7.2 Domain name dispute resolution through arbitration	12.48
12.13.7.3 Uniform Domain-Name Dispute Resolution Policy (UDRP)	12.48
12.13.8 The .IN Domain Name Dispute Resolution Policy (INDRP)	12.51
12.14 Linking and Framing	12.54
12.14.1 Linking	12.54
12.14.2 Trademark issues in linking	12.55
12.14.3 Framing	12.57
12.14.4 Trademark issues in framing	12.57
12.15 Meta tagging and Keyword Advertising	12.60
12.15.1 Metatags, keywords and search engines: an introduction	12.60
12.15.2 Metatagging and trademark infringement	12.65
12.15.2.1 Doctrine of initial interest confusion	12.65
12.15.2.2 Fair use defence	12.66
12.15.2.3 Position in India	12.67
12.15.3 Key word advertising and trademark infringement	12.68
12.15.3.1 Position in UK	12.68
12.15.3.2 Position in India	12.69
12.16 Conclusion	12.71

**Chapter 13 Digital brand management**

13.1 What is a Brand?	13.2
13.2 Digital Branding	13.2
13.3 Fundamentals for Digital Branding	13.3
13.4 Online Brand Management	13.4
13.4.1 Importance of digital brand management	13.4
13.4.2 Online reputation management	13.4
13.4.3 Tools for online reputation management	13.5
13.4.3.1 Website	13.5
13.4.3.2 Search engine	13.5
13.4.3.3 Social media	13.5
13.4.3.4 Review sites	13.6
13.5 Who is a Digital Brand Manager and why hire one?	13.6
13.6 What are Digital Assets?	13.6
13.7 Digital Brand Protection	13.8
13.7.1 Why do you need digital brand protection?	13.8
13.8 Case Studies	13.9
13.8.1 Zara controversy	13.9
13.8.2 D-Mart case	13.9

13.9	What are the techniques that can be used by the organisation to analyse market situation? .....	13.10
13.9.1	Social media .....	13.10
13.9.2	Google trends .....	13.10
13.9.3	Website audit .....	13.12
13.9.4	Marketing program .....	13.12
13.9.5	Social listening tools .....	13.12
13.9.6	Social analysis tools .....	13.13
13.9.7	Google Analytics .....	13.14
13.10	Avoiding Social Media Disasters .....	13.14
13.11	Search .....	13.15
13.11.1	Pay Per Click (PPC) and Search Engine Optimisation (SEO) relationship .....	13.15
13.11.2	Search engine .....	13.15
13.11.2.1	Google Operator .....	13.16
13.11.2.2	Google Search Console .....	13.16
13.11.3	Keyword researching for search engine optimisation .....	13.17
13.11.4	Difference between search engine optimisation (SEO), search engine marketing (SEM) and social media marketing (SMM) .....	13.18
13.12	Vulnerability Assessment and Penetration Testing (VAPT) .....	13.19
13.12.1	What is vulnerability assessment and penetration testing (VAPT)? .....	13.19
13.12.2	Importance of vulnerability assessment and penetration testing .....	13.20
13.12.3	Types of vulnerability assessment .....	13.20
13.12.3.1	Network based scans .....	13.20
13.12.3.2	Host based scans .....	13.20
13.12.3.3	Wireless network scans .....	13.21
13.12.3.4	Application scans .....	13.21
13.12.3.5	Database scans .....	13.21
13.12.3.6	Device penetration testing .....	13.21
13.12.4	Types of penetration tests .....	13.21
13.12.4.1	White box .....	13.21
13.12.4.2	Black box (blind test) .....	13.21
13.12.4.3	Hidden penetration test (double blind) .....	13.21
13.12.4.4	External penetration test .....	13.22
13.12.4.5	Internal penetration test .....	13.22
13.12.5	Difference between vulnerability assessment and penetration testing .....	13.22
13.12.6	Steps to conduct VAPT in an organisation .....	13.22

Internet law: regulating cyberspace and emerging technologies

13.13	Digital Footprints and Activities	13.23
13.13.1	What are digital footprints?	13.23
13.14	Brand Threat Assessment Report	13.24
13.14.1	What is brand threat assessment report?	13.24
13.15	Online Brand Monitoring	13.25
13.15.1	What is brand monitoring?	13.25
13.15.2	What should be monitored?	13.25
13.15.3	What should be tracked?	13.26
13.16	ISO Accreditations/ Standards	13.26
13.16.1	ISO/IEC 27000: Overview of information security management systems (ISMSs)	13.26
13.16.2	Why is ISO: 27001 certifications important?	13.26
13.16.3	What are the benefits of ISO: 27001 certifications?	13.27
13.16.4	Cases where brands got destroyed due to improper DBM	13.27
13.16.4.1	Bitcoin worth \$3 Million stolen from Coinsecure in April 2018	13.27
13.16.4.2	Snapchat and Snapdeal controversy	13.28
13.17	Good Practices to protect your tech and business information and keep it safe from Cyber Attacks	13.29

**Chapter 14 Privacy policy**

14.1	Categorisation of Data	14.3
14.1.1	Sensitive personal data or information [SPDI]	14.3
14.1.2	Personal data or information [PDI]	14.3
14.1.3	Major provisions involved	14.3
14.2	Mandatory Compliance	14.4
14.3	Non- Mandatory but Essential Compliance	14.6
14.4	Use of Visuals in Privacy Notices	14.9
14.5	Frequently Asked Questions	14.9
14.5.1	Public disclosure of information:	14.9
14.5.2	Aadhaar data	14.10
14.5.3	Security requirements	14.14
14.5.4	Consent	14.16
14.6	Sample Questionnaire to help you conduct Information Technology Audit in your organisation	14.17

**Chapter 15 New technologies and the law**

15.1	Artificial Intelligence	15.2
15.1.1	How does AI work and what are the technologies involved?	15.3
15.1.2	Artificial intelligence in law	15.4
15.1.3	Legal framework and its evolution	15.5

Table of contents

	15.1.4	Challenges of artificial intelligence	15.6
	15.1.5	Future of artificial intelligence in India	15.7
15.2		Internet of Things	15.8
	15.2.1	What is IoT?	15.9
	15.2.2	Applications of Internet of Things [IoT]	15.10
	15.2.3	Legal challenges to IoT	15.11
	15.2.4	IoT - International perspective	15.12
	15.2.5	Conclusion	15.13
15.3		Robotics	15.15
	15.3.1	Rise of internet	15.15
	15.3.2	Rise of automation and robotics	15.16
	15.3.3	The way ahead - internet to robotics and AI	15.18
	15.3.4	Law and robotics	15.19
	15.3.5	Conclusion	15.21
15.4		Blockchain	15.23
	15.4.1	Key legal and regulatory issues	15.24
	15.4.2	Virtual currencies, crypto currencies and crypto tokens	15.24
	15.4.3	Current uses of bitcoins in India	15.26
	15.4.4	Regulation of distributed ledger technology applications for financial services	15.26
	15.4.5	Legal framework	15.26
	15.4.6	Bitcoin is legal in USA	15.27
	15.4.7	European Union	15.27
	15.4.8	Japan	15.28
	15.4.9	Singapore	15.28
	15.4.10	Switzerland	15.28
	15.4.11	South Korea	15.28
	15.4.12	Taxation of transactions where consideration is paid in bitcoins, in India	15.28
15.5		Autonomous Vehicle	15.30
	15.5.1	Legal issues	15.31
	15.5.2	Risks and suggestions	15.32
	15.5.3	Who would be liable?	15.33
15.6		Drones	15.35
	15.6.1	Permits	15.35
	15.6.2	Remote ID and tracking	15.36
	15.6.3	Equipment requirements	15.36
	15.6.4	Flight restrictions	15.37
	15.6.5	Application process for licence of RPA System in India	15.37
	15.6.6	Six things to know before flying a drone in India	15.38