TECHNOLOGY LAW

Regulations, Cyber Policy, and the Digital Landscape

RODNEY D. RYDER
NIKHIL NAREN

Foreword by
Justice Sanjiv Khanna
Former Chief Justice of India

Introduction by
R Venkataramani
Attorney General for India

LAW & JUSTICE PUBLISHING CO

Edition 2026

ISBN:

Published by:

LAW & JUSTICE PUBLISHING CO

www.lawjusticepublishing.com

A-58, GT Karnal Road Industrial Area,
Delhi-110033
Phone: 011-47082254
sales@lawjusticepublishing.com

C-27, Connaught Place,
New Delhi-110001
edit@lawjusticepublishing.com

Distributors:

UNIVERSAL BOOK TRADERS
80 Gokhale Market, Opp. Tis Hazari Courts,
Delhi-110054
Phones: 011-23911966, 23961288
e-mail: sales@ubtlawbooks.com

Recommended Citation :
Rodney D. Ryder and Nikhil Naren, Technology Law:
Regulations, Cyber Policy, and the Digital Landscape
2026 Edition (New Delhi: Law & Justice Publishing Co.)

Printed at:

DEDICATION

For Rebecca, Mark, and Gunjan

–Rodney D. Ryder

For Yashita, my adorable niece [and our family's newfound joy!]—may you always walk your own path and dream in colour

–Nikhil Naren

ACKNOWLEDGEMENTS

This work is the product of many conversations—with students who asked difficult questions, colleagues who stress-tested arguments, professionals who shared frontline experience, and readers who insisted that legal analysis stay anchored to ground truth. We are grateful to our institutions and collaborators for the intellectual home they provided, and to our families for the patience that sustained long writing days. This text marks the start of an exciting, ongoing journey. We write to put on record our grateful thanks!

To our friends and families, thank you for your unwavering support and understanding during the long hours we spent on this work. Your patience and encouragement have been a constant source of motivation.

Our special thanks and gratitude to O.P. Jindal Global Institution of Eminence Deemed to be University, for its commitment to fostering innovative discussions and interdisciplinary approaches that significantly influence our work. With gratitude to the Hon'ble Vice Chancellor, Prof. (Dr.) C. Raj Kumar and the Hon'ble Registrar, Prof. Dabiru Sridhar Patnaik, for their visionary leadership and support in embedding the timely inclusion of the critical intersection of law and technology within the University and the legal academy, creating a pioneering niche for the Jindal Global Law School globally. We truly cherish our association.

We are deeply appreciative of and acknowledge the unwavering support of Shri Suneel Galgotia, Dr. Dhruv Galgotia, and Ms Aradhana Galgotia for their support and enthusiasm, which have been incredibly motivating.

We are profoundly grateful to the numerous universities and institutions that have provided us with the platforms to share our knowledge and insights on the intersection of law and technology. Your invitations to deliver lectures and conduct sessions have been invaluable in shaping the dialogue and understanding of this complex field. To all the students, faculty, staff, and professionals at these universities and institutions, thank you for your curiosity, insightful questions, and enthusiastic participation.

Our special thanks to all our colleagues and clients at Scriboard, with whom we have explored law and technology. The road is ever evolving [and challenging], but your wisdom and insights are unparalleled. For our esteemed clients, thank you for thinking of Scriboard as your first port of call.

Our special thanks to the students of law who assisted us with precise research in critical areas over the course of their one-month research assistantships in the past three years. We are grateful to [in alphabetical order]: Aaryan Dhasmana, Anushka Tatia, Ashita Mathur, Diya Sood, Gunjan Yede, Joshua Joseph, Kashish Gupta [also for the editorial assistance in the preliminary drafts], Prachi Chowdhury, Prithvika Survepalli, Ujjwal Gupta, and Yash Vardhan. While many of them are now professionals, they continue to remain students of law. Their attention to detail and efforts are commendable and appreciated.

Our special thanks to the Publishers, Law and Justice Publishing Company, for their tireless support and enthusiasm for the manuscript. Over the years, support from Pradeep ji, Sanjeev ji and Manish ji has been rock solid. After getting two editions of our book, *Artificial Intelligence and Law: Challenges Demystified,* published with them, we are delighted to have them on board to publish this text covering a broad and unparalleled avenue of *Law and Technology*. We are very grateful!

Our sincere thanks go to the concerned and dedicated officials at the Prime Minister's Office (PMO), the Ministry of Electronics and Information Technology (MeitY), the National Institution for Transforming India (NITI) Aayog, and the British High Commission, New Delhi. Their candid policy insights and publicly available materials were extremely useful.

Special thanks to the communities exploring this intriguing intersection of law and technology, whose ongoing dialogue and innovations inspired many of the discussions within these pages. Your work continues to push the boundaries of what is possible and necessary in this field.

Finally, to our readers, thank you for your interest in this book. We hope it provides valuable insights and contributes to the ongoing conversation about the intersection of law and technology. We humbly request the future readers [and users] of this book to share their feedback, constructive suggestions, views, and criticisms, if any, through any means of communication.

Rodney D. Ryder
rodney@scriboard.com

Nikhil Naren
contact@nikhilnaren.in
nikhil.naren@jgu.edu.in
nikhil@scriboard.com

ABOUT THE AUTHORS

Rodney D. Ryder

Founding Partner

Scriboard [Advocates and Legal Consultants]

Mr Rodney D. Ryder is a lawyer with over twenty-seven years of experience in Technology, Data Privacy, Intellectual Property, and New Media Law[s]. He is the Founding Partner of Scriboard, a full-service commercial law firm with cutting-edge specialisation 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 studied History at St. Stephen's College, University of Delhi, where he obtained the University Gold Medal for the highest aggregate score. At College, he was awarded the Wescott Memorial History Prize, the TG Percival Spear Memorial Prize and the Dip Chandra Medal, amongst other prizes. Mr Ryder studied law at the Campus Law Centre, University of Delhi and was called to the Bar in India in the year 1998.

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.

Mr Ryder has been nominated as a 'Leading Lawyer' in intellectual property, technology, communications, and media law by Asia Law, Who'sWhoLegal, Asia Legal 500, amongst other International publications. Mr Ryder has been listed as one of India's leading lawyers in the '40 under 45' study conducted by Who's Who Legal, United Kingdom. Mr Ryder was listed in 'Super 50 TMT' list of leading TMT lawyers in Asia published by Asian Legal Business.

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

judgment by the Hon'ble Supreme Court of India on domain names [*Satyam Infoway Ltd.* v. *Siffynet 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.

He has been and is Adjunct Professor/Visiting Faculty to the Campus Law Centre, Faculty of Law, University of Delhi, the CBI Academy, the Indian Institute of Management, Lucknow [IIML], the Indian Institute of Technology, Kharagpur, the Institute for Development and Research in Banking Technology, Hyderabad, NALSAR, Hyderabad, the National Law School of India University [NLSIU], Bangalore, the National Law University [NLU], Jodhpur, and Symbiosis Law School[s] – NOIDA/Pune/Hyderabad.

BOOKS

- "Guide to Cyber Laws [E-commerce, the Information Technology Act, 2000, Data Protection and the Internet]". {LexisNexis Butterworths Wadhwa Nagpur, India}. Third Edition 2007.
- "Intellectual Property and the Internet". {LexisNexis, 2002}.
- "Brands, Trademarks and Advertising". {LexisNexis, 2004}.
- "Drafting Corporate and Commercial Agreements: Legal Drafting Guidelines, Forms and Precedents"; {Universal Law Publishing, 2005; Reprint 2007}
- "Right to Information – Law, Policy and Practice". {LexisNexis Butterworths Wadhwa Nagpur, India, 2006}.
- "An Introduction to Internet Law and Policy: a course book on cyber law". {LexisNexis Butterworths Wadhwa Nagpur, India, 2007}
- [With Ashwin Madhavan] Intellectual Property and Business: The Power of Intangible Assets. {Sage Publications. 2014}
- [With Ashwin Madhavan] Cyber Crisis Management: Overcoming the Challenges in Cyberspace. {Bloomsbury. 2019}.
- [With Nikhil Naren] Internet Law: Regulating Cyberspace and Emerging Technologies. {Bloomsbury Professional India. 2020}
- [With Nikhil Naren] Artificial Intelligence and Law: Challenges Demystified. {Law and Justice Publishing Company. 2022; Second Edition. 2024}

He can be reached at- rodney@scriboard.com

Nikhil Naren

Chevening Scholar

Assistant Director, Cyril Shroff Centre for AI, Law and Regulation; Assistant Professor, Jindal Global Law School

***Of Counsel*, Scriboard [Advocates and Legal Consultants]**

Mr Nikhil Naren is a class of 2022 graduate of Queen Mary, University of London, where he pursued his Master of Laws [LL.M.] specialising in Technology, Media and Telecommunications law as a Chevening Scholar, and a Bachelor of Arts and Bachelor of Laws [B.A.LL.B.] graduate from the class of 2020 of Symbiosis Law School, NOIDA, Symbiosis International (Deemed) University, Pune. He also 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 the Federation of Indian Chambers of Commerce and Industry (FICCI), New Delhi.

Mr Naren is presently an Assistant Professor at the Jindal Global Law School (JGLS) and Assistant Director, Cyril Shroff Centre for AI, Law and Regulation in Sonipat, Haryana, on the side, being an *Of Counsel* at Scriboard [Advocates and Legal Consultants], New Delhi. At JGLS, he has taught the courses- *Regulation of Technology and Cyberspace* [also the Course Convenor], *Moot Court and Trial Advocacy*, and *Drafting, Pleading, and Conveyancing* to the undergraduate students of law. At the postgraduate level, he has taught the course- *New Technology and Intellectual Property, Artificial Intelligence* and developed and taught the course, *Regulation of Artificial Intelligence: Challenges and Opportunities*. Besides these courses, Mr Naren has in the past taught an elective course, *Rethinking Technology Law in the Digital Era* and is presently teaching his elective course, *Regulating Artificial Intelligence,* to a diverse class of students.

Mr Naren has also been a Former Consultant with the Digital Economy Capacity-Building Section at the United Nations Conference on Trade and Development [UNCTAD]. It is worth mentioning that Mr Naren is also one of the youngest awardees of the prestigious and highly coveted British Chevening Scholarship from India. Recognised for his dedication beyond academics and professional work, he was one of the seven Chevening Scholars from his cohort, out of a total of 1600 scholars from close to 140 countries, to receive the 'Gold Award' from the Chevening Secretariat and the Foreign, Commonwealth, and Development Office, for dedicating over hundred hours of volunteering in the UK—a testament to his commitment to community service. During his time at Queen Mary, he also worked under the guidance of Prof. Christopher Millard on the *Microsoft*-funded

'Cloud Legal Project' as a Teaching Associate. He also advised [*pro bono*] a UK-based Agri-Tech start-up and assisted them primarily with contract reviews, contract drafting, intellectual property strategy, brand protection and management, market research, operations and strategies, data protection compliance, etc.

Leading law schools and organisations regularly invite him to deliver corporate training sessions or teach various aspects and the impact arising out of the intersection of law and technology. Upon invitation, Mr Naren has delivered a session on *Artificial Intelligence* at the Headquarters of HCLTech, a session on the *Adoption of Artificial Intelligence in Legal Processes* at the Luthra & Luthra Law Offices, and has also trained Accounts and Audit Officers from the Office of the Comptroller and Auditor General of India.

Upon invitation, Mr Naren has designed and taught a credit course, *Legal Foundations for Technology, Innovation, and Entrepreneurship*, at the National Law University, Odisha, and at the West Bengal National University of Juridical Sciences, Kolkata. He is also a visiting faculty at the National Law University, Delhi, where he is teaching his Seminar Course, *Artificial Intelligence and Law: Navigating the legal frontiers.*

Mr Naren is a distinguished scholar and has carved a name for himself in the intersection of law and technology at an early age. He is the co-author of the book- *Internet Law: Regulating Cyberspace and Emerging Technologies*, published by Bloomsbury and two editions of *Artificial Intelligence and Law: Challenges Demystified*, published by Law & Justice Publishing Company, which is one of the first books on the subject matter by Indian authors.

Mr Naren continues to contribute opinion pieces in renowned national dailies such as LiveMint, The Hindu, The New Indian Express, Firstpost, News18, The South First, among others. After receiving a record Pre-Placement Offer (PPO) from Scriboard, Mr Naren has advised leading Social Networking, e-Commerce, Public Sector Undertakings, Start-Ups, and Fortune 100 and 500 companies on handling disputes and maintaining compliances pertaining to the Information Technology Act of 2000 and the Rules made thereunder, Intellectual Property, Contractual Disputes, Brand Management, Privacy and Data Protection, and Emerging Technologies.

Mr Naren has also been an avid mooter during his law school and endeavours to contribute to this space in his spare time. He has drafted problems and judged two editions of Chanakya National Law University's National Cyber Law Moot Court Competition, NIMS University Corporate and Commercial Law Moot Court Competition and the University of Petroleum and Energy Studies's ADR Competition-Madhyastham's final rounds. He has also been invited to judge various co-curricular competitions by Symbiosis Law School, Maharashtra National Law University, Mumbai; Himachal Pradesh National Law University; Narsee Monjee Institute of Management Studies; Galgotias University; the International Bar Association's International Criminal Court Moot Court Competition; the Philip C. Jessup International Law Moot Court Competition; and the Brown Mosten International Client Consultation Competition.

He can be reached *via* email at- contact@nikhilnaren.in; *LinkedIn*- Nikhil Naren; and *Instagram*- @nikhilnaren.in.

ABOUT SCRIBOARD [ADVOCATES AND LEGAL CONSULTANTS]

www.scriboard.com

Scriboard [Advocates and Legal Consultants], New Delhi, is a full-service commercial law firm with cutting-edge specialisation in Information Technology, Data Privacy, Cyber Security and Intellectual Property. The firm was founded in the year 2010 by Rodney D. Ryder, a leading technology, data privacy, and intellectual property lawyer.

Over the past decade, Scriboard has been listed consistently as a leading law firm in intellectual property, technology, communications and media law by Asia Law, Who's Who Legal, Chambers, Managing Intellectual Property, Asia Legal Business, Asia Legal 500, amongst several international publications.

The firm is legal counsel to the Ministry of Communications and Information Technology, Government of India and to the National Internet Exchange of India [NIXI], which manages the .in [Indian Country Code Top Level Domain Extensions]. Scriboard is also counsel to leading technology companies like Amazon, Hike Private Limited, and Stripe, Inc. At the national and international level, the firm has represented leading companies and individuals, including the IndianOil Corporation, Godrej Consumer Products Limited, ITC Limited, Havells India Limited, FanCraze, and the former Indian cricket captain Shri Mahendra Singh Dhoni.

The firm also advises the Central Bureau of Investigation [CBI] on Internet Security and Cyber Crime. The firm services clients in Nepal, Bhutan, Bangladesh, Pakistan and Sri Lanka. The firm acts as a legal advisor to the Computer Association of Nepal [CAN], the Nepal Supreme Court and the Nepal Telecom Authority [NTA]. In addition, the firm has assisted the government in Nepal in drafting and preparing the Electronic Commerce Law.

ABOUT METABOARD:

www.metaboard.com

MetaBoard® [www.metaboard.com] is a learning, development, and training service. MetaBoard® functions as a platform and a service to empower individuals from all walks of life and work to use the law, technology, artificial intelligence and related learning tools.

MetaBoard® is many things at once: a legal tech platform, a consulting service, and a connector connecting experts in law education and management to offer innovation and solutions that drive transformation.

FOREWORD

SANJIV KHANNA
FORMER CHIEF JUSTICE OF INDIA

For millennia, law has provided the foundation upon which humanity has organised its collective life. From the *Arthashastra* in the East to the Magna Carta and the civil codes in the West, societies sought to govern, regulate personal relationships and resources through rules rooted in territory and enforced within boundaries. These structures with government oversight and enforcement are the core of legitimacy and Rule of Law.

Driven by creativity and innovation, the rise of cyberspace has upended this paradigm. With a device small enough to fit in the palm of a hand, an individual can traverse continents, reach millions, and access information and entertainment instantaneously. The borderless virtual world fosters "marketplace of ideas" and unleashes business opportunities on a scale never before imagined, while at the same time confronts the law with complexities more profound than any it has previously known. The traditionally understood structured body of principles and institutions designed to regulate conduct, behaviour, and safeguard social order are challenged as the wrongdoers exploit anonymity, distances and borders, and technological and legal loopholes.

The task before the law and institutions is to extend its reach into cyberspace and to adapt in ways that preserve accountability, and at the same-time sustain the freedom and autonomy that define the digital age.

In India, the Information Technology Act, 2000 provides the legislative foundation for cyberspace regulation. One of its most significant contributions lies in granting legal recognition to electronic records and digital signatures, thereby placing them on par with traditional paper-based documents. This marked a decisive shift in evidentiary and contractual practices, ensuring that the law kept pace with technological change.

Beyond recognition of digital records, the Act addresses a wide spectrum of concerns: admissibility of electronic evidence in judicial proceedings, standards of cybersecurity, protection of personal data, and obligations relating to storage and maintenance of electronic records. Collectively, these provisions establish a comprehensive legal architecture that continues to evolve in response to new technological challenges

This book undertakes a critical examination of the legal and human dimensions of cyberspace. It engages with questions of free speech and its limits, the rise of digital defamation, competing jurisdictional theories, and the emerging framework

of data protection laws. These issues are analysed with an appreciation of both doctrinal principles and their practical implications in the digital sphere.

The role of social media is addressed in the chapter *Like, Share but Be Aware.* It highlights how platforms that foster connectivity also enable manipulation through social engineering, proliferation of fake accounts, large-scale data leaks, and misuse of personal information. The chapter further examines the growing influence of online personalities and the risks associated with beguiling digital expression. Emphasis is placed on the need for vigilance, informed participation, and preventive strategies to safeguard users in this dynamic environment.

The book also turns to intellectual property in the digital age, where copyright, trademarks, and domain name disputes acquire new complexity. Emerging phenomena such as meme culture, deepfakes, and meta-tagging are examined not only as cultural shifts but also as legal challenges, raising questions about authorship, ownership, and protection strategies in an online environment.

Equally significant is the question of digital branding. The discussion simplifies concepts such as brand management, online reputation tools, market analytics, vulnerability assessments, and brand threat reports, explaining how they shape identity and trust in the virtual marketplace. These analyses underline the growing importance of safeguarding both personal and commercial reputation in a borderless digital economy.

Another focal point is surveillance, explored in Chapter 5 aptly titled *Who is Watching You.* It scrutinises the expanding powers of state surveillance, juxtaposed with constitutional guarantees of privacy and liberty. The chapter reflects on the need to preserve the delicate balance between national security imperatives and individual rights, an equilibrium that lies at the heart of every democratic society.

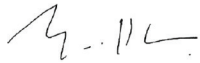
Contemporary concerns such as the *Right to be Forgotten* are analysed in detail, situating the concept within present-day debates on privacy, autonomy, and the permanence of digital memory. By tracing judicial and legislative developments, the discussion underscores the tension between individual rights and the collective interest in preserving information.

The book also turns to the architecture of digital governance. It examines government-to-citizen and government-to-business initiatives, with particular reference to the Aadhaar case, and highlights how technology can both empower and unsettle democratic governance. Real-world applications are used to illustrate the promise and perils of large-scale digital identification and service delivery systems.

Finally, the growing domain of e-commerce is addressed in the chapter *From Clicks to Carts.* It explores the legal dimensions of electronic contracts, intermediary liability, consumer protection, and deceptive online practices often described as "dark patterns." By unpacking these intricacies, the chapter offers a nuanced understanding of the regulatory framework that governs digital transactions and its implications for both businesses and consumers.

Taken together, the themes explored in this book reflect both the transformative potential of technology and the formidable challenges it presents. Cyberspace is not simply a new platform of interaction. It is a domain that compels the law to evolve with unprecedented speed, while remaining anchored in the principles of liberty, accountability, and fairness.

This work succeeds in capturing that reality. It will serve as a guide to the complexities of digital regulation and as a reminder that the Rule of Law must remain the touchstone of our digital future. I have no doubt that scholars, practitioners, policy-makers, and students alike will find in its pages insight, clarity, and inspiration to meet the challenges of an ever-expanding digital world.



Sanjiv Khanna

New Delhi;
August 25, 2025.

सत्यमेव जयते

R. Venkataramani
Attorney General for India

SE-127, Law Officers' Chambers, 2nd Floor
Supreme Court of India, New Delhi - 110001
Tel.: 23383254

INTRODUCTION – FROM THE DESK OF ATTORNEY GENERAL FOR INDIA

1. Information sustains life. Information both connects and disconnects. Our minds, like the brains of all conscious beings, gather, attend to and share information. There is an evolutionary need in all these at the species level. It is said that a sea slug, "which has one of the basic nervous systems on earth and no consciousness to speak of, will respond to the sudden presence of threat stimuli." At the social level, there are other dimensions to information, sharing and connections. Only the way we gather, or collect information and share, has differed over the ages. The printing press pushed us into a more speedy and permanent way of communication. The radio waves gave us an enlarged spread of communication. The further explosions of electronics and cyberspace have made our collection and sharing of information fundamentally different from earlier machine ages. When technology has become our mind as if our brains are disabled in functioning without their aid, we are now talking about the principles of individual, collective, national and global management of our lives on the laps of technology, and to innovate on regulatory and punitive new brave worlds. Every law and every regulation in the emerging cyberspace and data regimes have to struggle to invent anew as dark forces and evil geniuses seem to be scoring challengingly.

2. The range of information has expanded, from business and commerce to science and technology, to culture and arts, to education and public information, which is the pulp of all communication today. No information can ever remain within anyone's chest, nor can unshared information have any value. Sharing begets economic, political and social interactions and all those exchanges which add sense and value to our lives. But who shares what, for which ends, and how can emanation and means of pursuit of wrong ends be dealt with are questions which are deeply embedded in technology that regulation is left gasping. The new machine age is an age with instant, sometimes irreversible and seismic impacts on our lives, individual and collective. So it is we are now called upon to engage in talk about all of them

to understand the limits of our current ideas in law about handling, preventing, correcting or remedying wrongs in the physical space and to extend them to the invisible space.

3. The book is an ambitious attempt to understand this engagement. Walking on nascent terrain is challenging, and I should say that the authors have successfully measured the landscape they have set out to explore. The landscape they have covered, besides being wide, is thoughtful and intrinsically connected.

4. Stories, anecdotes, chronicles, and thus portraits of history are powerful information tools. Confidentiality, secrecy, and privacy are involved in these. So, we have today a technology spread that has dimensions and aspects beyond conventional physical space phenomena. How do we unravel all these for common readers and professionals who need a guide, a companion in case of doubts, and an exhaustive reference library? The book answers these questions.

5. Ever since George Orwell wrote "1984", the idea of a thought machine has caught the imagination of scientists, technologists, and social theorists. The chapter on "who is watching you", understanding surveillance, is a brief but substantial portrayal of both the technology of watch and the state and private players as watchmen without our consent. It is a capsule comprehension of the sprawling literature on the subject.

6. Free speech and social security have entered new combats. The communications and cyber space technology has opened up doors for free communication without the watchful and weeding eyes of editors. But the emerging freedom has produced nightmares and free-roaming stallions of expression, unrestrained in content and language. The web and range of liabilities for wrongful speech (such as defamation) are given to us in simple narrations in this chapter. Responsibility of cyberspace providers is now a well-documented subject, and who can hold whom responsible for what will continue to be debated and subjected to judicial scrutiny. Rightly have the authors dealt with the question of jurisdiction in a connected way in the same chapter, though this question of remedial challenges in general are dealt with in other chapters.

7. Chapter 7 again takes us on a global journey into digital data protection. As we saw, data is the backbone of everything we do. Can any data be sold and bought for a price in a market designed freely and operated freely beyond any regulation? Can our data be stored and used by the State for reasons which may be legitimate at one level but open to abuse? This chapter peeps into these questions and asks us to ask more questions. The comparison of Indian data protection law and European standards, which are comprehensive, is instructive.

8. Privacy talk is now a staple legal talk. Privacy has undergone mutations. It is now an umbrella of sorts. Chapter 6 is a brief survey of this attractive subject. It

covers the journey of the Indian data protection law to open up to the continued engagement on the new paths of "data civilisation", if one may use that expression. Chapter 14 quickly introduces us to privacy policies and again asks more questions. E-commerce is another pathway for social and economic communication. It has changed our ways of doing business and the speed of transactions. We cannot reverse this or abandon the connectivity treasure house. With freedom in cyberspace comes the governance question. This is entangled with the entire cyberspace, and all regulatory questions necessarily arise. E-Governance is not merely making economic life simple, but also a matter of State power. A brief survey of government engagements in this domain adds to what citizen assistance governance will be called upon to do.

9. Exploration of the boundaries of competitive secrecy and confidentiality in the domain of ideas, which is what intellectual property is about, is an expanding subject. The reference to "John Doe's orders" and their potential as useful judicial tools in chapter 12, while exploring intellectual property protections, is a good stimulant. Chapter 12 is exhaustive and covers the entire canvas of intellectual property protections in the age when the frontiers of trespass and entry into protected spaces have broken down.

10. Way back in 2001, a hugely informative and critical work titled "Law and Information Technology" was published. (Law, information, and information technology, edited by Eli Lederman and Ron Shapiro.) As I sat down to pen my introduction, I remembered the sweep of the contents of that book. I find a good deal of similar endeavour in this book.

11. Social media's duality, as a freedom-enabling domain and a dark room for wrongs, is itself a multidimensional subject of study. Chapter 11 broadly traverses the injurious use of social media, such as social engineering, the trade of illegal products, fake accounts, information leaks, etc. There is much more to be dealt with on this subject. It is also seen that given the overlap of areas of cyberspace, many wrongs are interlinked.

12. Without a peep into cybercrimes, a book of this genre would have been incomplete. Chapter 2 succinctly deals with this issue. Books on cybercrimes are increasing in proportion to the increase in cybercrimes. This chapter provides a quick guide on the new penal legislation and the information technology law dealing with cybercrimes.

13. Finally, chapter 15, by simple statements and illustrations, including international perspectives, and the Internet of Everything, discusses the imperative of unorthodoxly paying greater attention to social and legal regulation. It is a good end to capture the broad threads of an otherwise endless stream of subjects. I congratulate the authors for their imaginative and elegant exposition of the subjects

and for providing the necessary links between the apparently distinct aspects of emanations of cyberspace. The book can be treated as a textbook, an information spreadsheet, a legal primer, and an explorer. I wish that authors would continue to produce more work of this genre.

R. VENKATARAMANI
ATTORNEY-GENERAL FOR INDIA

NEW DELHI
15.10.2025

PREFACE

Why this book, and why now?

Technology no longer sits at the edges of law; it writes the fact patterns lawyers argue about, it shapes the evidence courts examine, and it determines the rights individuals can meaningfully exercise. Payment rails nudge spending, search engines steer attention, "smart" systems profile behaviour, and platforms convert identity into inventory. In such a world, the vocabulary of law [consent, liability, authorship, due process], must learn to speak fluently with the vocabulary of "code" [data, models, protocols, optimisation]. This book is our attempt to build that shared language.

The Prologue sketches the social arc: how velocity in innovation has amplified visibility, risk, and responsibility. This Preface sets out the project's legal arc: a practical, doctrine-aware, technology-literate guide to navigating disputes and decisions that are already here, not hypotheticals waiting for some distant future.

What this book tries to do [and not do]

We have written for readers who need clarity without oversimplification. You will find:

- Black-letter anchors where the law is settled, and reasoned pathways where it is not.
- Doctrinal analysis tied to product realities: how an app collects data, how a model is trained, how a domain is taken down, how evidence is preserved and challenged.
- Comparative signposts to global frameworks [for example, how different countries approach data protection] alongside India's fast-evolving regime in data protection, electronic evidence, intermediary liability, etc.

What you will not find are cut-and-paste checklists divorced from context. A privacy notice or a privacy policy, for instance, is no longer a template exercise; it is a living contract of data practices that must be defensible before regulators, Courts, and the Court of public opinion.

The Blueprint

We begin with the legal spine of India's digital order: the *Information Technology Act, 2000*—its origins in national and international trade imperatives, the adjudicatory design for penalties and compensation, and the 2008 amendment that reshaped

compliance obligations. This opening does not shy away from critique: it examines what the IT Act does well, and where enforcement has struggled against modern vectors like spam, phishing, cyberwarfare, and IP infringement, before setting out our proposals and the policy debate around the mooted *Digital India Act*.

From first principles, we move into the realities of cybercrime—hacking, denial-of-service attacks, phishing, cyberstalking, revenge pornography, and software piracy, treating them not as headlines but as chargeable, evidence-dependent offences. Here, identity theft and tampering with computer source code are unpacked element by element, and the chapter situates domestic law alongside reference frameworks such as the *Tallinn Manual* and high-salience incidents like the *Ukraine grid attack*. A dedicated Standard Operating Procedure translates statutory text into operational steps for investigators and counsels.

Recognising that digital disputes rise or fall on proof, electronic evidence receives its own doctrinal treatment: Section 65B's afterlife within the *Bharatiya Sakshya Adhiniyam*, the contours of admissibility for everything from hard disks and compact discs to call recordings, presumptions, and the role of forensic examiners. This is a practitioner's map for keeping the chain of custody intact while preserving the flexibility to litigate evolving formats.

With security, we eschew buzzwords for mechanics. Malware analysis [static, dynamic, and hybrid], antivirus detection approaches [signature, behaviour, and specification], and network defences [packet filters to stateful firewalls] are translated into legal risk language: what is "reasonable" security, what belongs in a due-diligence file, and where liability can hinge on understanding how profiling, IP addresses, and email systems actually work. The chapter closes with sober threat summaries—malware, intrusion, and messaging-layer abuse.

The next movement tracks the law of interception, blocking, and monitoring—Sections 69, 69A, and 69B of the IT Act—against the constitutional right to privacy. We reconstruct the case for and against these powers, including the standards and process for blocking orders, *CERT-In* reporting under Section 70B, and the burden of retention placed on intermediaries. The encryption debate is handled on its merits: what technical weakening means in practice, and what trade-offs are defensible in a rights-respecting democracy.

Having framed surveillance, we turn to privacy as a positive architecture of rights: bodily, decisional, informational, and communications privacy; landmark jurisprudence; and the frictions with speech and transparency. The analysis spans common-law remedies [confidence, trespass, nuisance] and modern statute, culminating in a guided comparison of the *General Data Protection Regulation* [GDPR] and India's framework, including the right to be forgotten and the way telecom-sector regulation intersects with private life.

A companion chapter then refracts the *Digital Personal Data Protection Act, 2023,* through a global lens. It traces legislative history, clarifies scope, and builds a

compliance grammar around notice and consent, the obligations of Data Fiduciaries [ordinary and Significant], breach notification, Data Protection Officers, and the jurisdiction of the Data Protection Board. Side-by-side comparisons with Australia's *Privacy Act*, China's *Personal Information Protection Law*, European Union's GDPR, Singapore's *Personal Data Protection Act,* the United Kingdom's-GDPR, and the United States sectoral laws—and a topical survey of the most recent *UK's Data (Use and Access) Act, 2025*—show where India converges, where it experiments, and where gaps remain.

With rights and data foundations in hand, the book confronts speech, defamation, and jurisdiction online. It canvases constitutional protections and "reasonable restrictions," then drills into intermediary liability [Section 79 and the IT Rules, 2021], limitation issues, and adjudicatory choices. A comparative walk-through of jurisdictional tests—long-arm statutes, effects doctrine, minimum contacts, specific vs general jurisdiction, equips readers to brief cross-border cases without mystique, alongside India-specific procedural anchors in the *Code of Civil Procedure*, *Code of Criminal Procedure/Bharatiya Nagarik Suraksha Sanhita*, *Indian Penal Code/Bharatiya Nyaya Sanhita,* and Intellectual Property statutes.

E-governance is treated as a living practice: the recognition of e-records and e-signatures, *DigiLocker's* trust model, and service archetypes [G2C, G2B, G2G, G2E] connected to policy frameworks like the *National e-Governance Plan*. A case study on *Aadhaar* surfaces the persistent tension between scale, inclusion, and data minimisation—preparing readers for the compliance and litigation themes that recur throughout the book.

Commerce receives a thorough, technically grounded treatment in the chapter on e-Commerce [from clicks to carts]: UNCITRAL's influence, business models [B2B to G2C], EDI, the cryptography behind digital and electronic signatures, and their legal standing. Intermediary liability is explored through leading Indian cases; consumer protection brings dark patterns into sharp relief; and electronic contracts are unpacked from offer and acceptance to attribution and time/place of dispatch. The chapter closes with India's open-stack experiment—*Open Network for Digital Commerce*—as a test of platform neutrality, competition, and standards.

The chapter on social media [Like, Share, but be Aware] turns the lens to people and platforms: social-engineering life cycles, fake-account forensics and verification, prevalent social-media crimes, and the anatomy of data leaks [with organisational and consumer impacts]. Privacy topics such as voyeurism, data retention, and sharenting are grounded in real-world harm, while spyware and spam apps preview the compliance questions that in-house teams face daily. The section on social-media "clickstars", our deliberate alternative to "influencers", considers their civic and political salience and the rights-based constraints that should shape platform and state responses.

The IP trilogy—copyright, trademark, and domain names—is written for the age of remix and automation. We revisit exclusive rights in code, fair dealing/fair use, *John Doe* orders, memes and deepfakes, then march through trademark fundamentals to online infringement, dilution, and *passing off*. Domain name disputes are treated as a first-resort Internet remedy, with anatomy, registration, and proceedings under the *Uniform Domain-Name Dispute Resolution Policy* [UDRP] and *.IN Domain Name Dispute Resolution Policy* [INDRP], plus Indian case law and modern controversies around linking, framing, metatags, and keyword advertising across the United Kingdom and Indian positions. We have supplied a wealth of examples from our law firm's practice on domain name disputes.

Modern brands are built [and broken] online, so Digital Brand Management receives a practitioner's manual: defining digital assets, structuring *Online Reputation Management*, and stress-testing with case studies [from FMCG missteps to crypto exchange losses]. We cover market-listening stacks [search, social, audits], *Pay-Per-Click/Search Engine Optimisation* strategy and its litigation implications, *Vulnerability Assessment and Penetration Testing* as governance, not theatre, digital footprints, brand-threat assessments and monitoring, and ISO/IEC 27001. The chapter ends by mapping good practices and the complicated role of social-media clickstars in reputation arcs.

Because policies are now product features, Privacy Policies are rebuilt from first principles: data categorisation, mandatory and essential compliance elements, visual design of notices, and frequently asked questions [including a careful subsection on *Aadhaar*]. We include a field-tested IT audit questionnaire so that teams can translate policy into verifiable controls.

The book closes with emerging technologies—Artificial Intelligence, Internet of Things, robotics, blockchain and crypto, autonomous vehicles, drones, and online gaming—not as futurism but as live dockets. Each sub-chapter pairs technical primitives with legal questions: explainability and allocation of responsibility in AI; device security and liability in IoT; governance choices for distributed ledgers across jurisdictions [and taxation in India]; fault and insurance in autonomy; flight licensing and ceilings in drones; and the knotty, still-contested divide between games of skill and chance in online gaming, with advertising standards and taxation folded in.

Taken together, these chapters build a single capability: to see how code, markets, and institutions co-produce legal risk, and to answer, with doctrinal discipline and technical literacy, the question that animates every dispute and design decision in technology law: who decides, on what data, under whose safeguards, and to what end?

As Co-Authors, this book is written in the first-person plural. However, when we speak of 'we', we may be referring, variously, to our joint views or experience, or either of us.

Happy Reading!

Rodney D. Ryder

Nikhil Naren

PROLOGUE

Before this book found its shape, it lived through drafts, detours, and doubts. The words of *Theodore Roosevelt* in his "Citizenship in a Republic" speech[1] steadied my hand—

> *"…It is not the critic who counts; not the man who points out how the strong man stumbles, or where the doer of deeds could have done them better. The credit belongs to the man who is actually in the arena, whose face is marred by dust and sweat and blood; who strives valiantly; who errs, who comes short again and again, because there is no effort without error and shortcoming; but who does actually strive to do the deeds; who knows great enthusiasms, the great devotions; who spends himself in a worthy cause; who at the best knows in the end the triumph of high achievement, and who at the worst, if he fails, at least fails while daring greatly, so that his place shall never be with those cold and timid souls who neither know victory nor defeat…"*

These lines, which are more commonly referenced as the "Man in the Arena" speech, became my compass for this book and my journey of navigating the crucial intersection of law and technology. If this book achieves anything, let it be the courage to do the work in public—to err, to learn, and to press on until the ideas are ready to stand on their own. Finally, the manuscript has stepped out of the workshop and into the 'arena'.

From my earliest days in law school in 2015, I was captivated by how technology quietly rewrites the rules of everyday life. I chose technology law when there were few takers and even fewer templates, not because it was 'popular' but because the questions were urgent. What *Stuart Russell*, in his book "Human Compatible", aptly refers to modern threats of AI machines to humanity as the "Gorilla problem", my thoughts were: Who is accountable when technologies err? How do we protect human dignity and due process in systems that move at machine speed? Can we regulate technologies or cyberspace *effectively*? Back then, the choice raised eyebrows; today, as the domain has grown, some call me "lucky". But over a period of time, I have come to a realisation that luck is nothing else, but a simple conviction that is practised early and often. On a lighter note, I began working at the intersection of *Artificial Intelligence and Law* in 2020, while remaining hopeful about the

1. Address at the Sorbonne in Paris, France: "Citizenship in a Republic". Retrieved from https://www.presidency.ucsb.edu/documents/address-the-sorbonne-paris-france-citizenship-republic.

opportunities and my curiosity about what the integration of data protection and AI systems would play out or if ever AI could create 'novel works' with minimal or without human input. While I was worried for the future and how these new issues are going to challenge the limits of the law, I was suggested to pick a "safer" topic; the running joke now is that I just showed up early to the party. In 2022, my *Guru* [Mr Rodney Ryder] and I co-authored one of the first books by Indian authors on this critical intersection, which got its second edition in 2024 [and the work on the next one will soon be underway].

I am still unsure if my optimism to pursue the intersection of law and technology stemmed from my belief in *Yhprum's law*, but those early bets taught me two habits I commend to today's students or professionals [of course, with a take it or leave it choice!]: persevere when a field is unfashionable, and learn to spot weak signals of the future before they become headlines. Read statutes, yes, but also read product roadmaps, terms of service, and the incentives that technology creates. It is time to cultivate interdisciplinary curiosity and the patience to do unglamorous work that builds real expertise. If you show up consistently and keep your compass fixed on people and the public interest, the future will not merely happen to you; you will help draft it.

We live in an extraordinary era, marked by unprecedented and immediate access to people, information, and content across the globe. Technology has fundamentally reshaped how we communicate, govern, trade, and entertain, offering remarkable growth, visibility, and transparency. Yet, the very features that empower us can also render our digital landscape fraught with vulnerabilities. This book, *Technology Law: Regulations, Cyber Policy, and the Digital Landscape*, is an essential guide designed to help readers comprehend, navigate, and critically assess both the potentials and pitfalls inherent in our digital age.

Consider the phenomenon of content creation, once confined to niche audiences but now powerful enough to influence public opinion instantly and globally. Platforms amplify individual voices and visibility irrespective of geographical boundaries, often without sufficient oversight. The shutdown of *Omegle*, whose CEO cited "psychological unsustainability"[2], vividly illustrates the urgent need for stringent platform regulations. This theme aligns seamlessly with the discussions in our chapters on Social Media and Emerging Technologies, highlighting platform responsibilities and user protection.

Recent global initiatives, such as Australia's implementation of age-gating policies on social media[3], reflect growing concerns about children's exposure to harmful content and vulnerable language. Such proactive measures underscore

2. BBC, Omegle shut down: Video chat website closed after abuse claims. Retrieved from https://www.bbc.com/news/business-67364634.
3. eSafety Commissioner-Australian Government, Social media age restrictions. Retrieved from https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions.

essential governance practices explored deeply in our chapters on Privacy Policy and E-Governance. E-Governance has emerged as one of the most transformative promises of technology, enabling governments to move beyond bureaucratic inertia toward transparent, efficient, and citizen-centric service delivery. From digital identity systems to online grievance redressal, technology has redefined the state–citizen interface, reducing barriers of time, geography, and access. Yet, the effectiveness of e-governance depends not only on the deployment of sophisticated platforms but also on the inclusivity, accountability, and data protection frameworks underpinning them. As this book explores in its dedicated chapter on E-Governance, the challenge is to ensure that digital tools do not simply replicate old hierarchies in new forms, but instead truly democratize governance, foster trust, and safeguard the rights of citizens in a rapidly digitising world.

Technology has also created unconventional careers, for instance, turning meme-making into a digital marketing skill. Yet, this seemingly benign trend brings forth complex ethical, legal, and social issues detailed in our chapters on Intellectual Property and the Internet, and Digital Brand Management. Within this shifting landscape, the necessity of digital brand protection cannot be overstated. A brand's online presence today is often its greatest strength and its greatest risk. From cybersquatting and counterfeit sales to social media impersonation and misleading advertisements, threats to brand integrity are multiplying at a pace unmatched by traditional regulatory tools. Protecting digital brands is not only about safeguarding intellectual properties; it is about preserving consumer trust, ensuring fair competition, and maintaining the reputational capital upon which modern commerce depends. The chapters on Intellectual Property and the Internet and Digital Brand Management also demonstrate how proactive strategies and legal safeguards can shield brands against misuse while enabling innovation to flourish.

Similarly, technology-driven freelancing represents an economic shift, highlighting both opportunities and the necessity for thoughtful, balanced regulations, as detailed in our chapters on E-Commerce and Social Media. We have argued that the term "influencer" carries a hazard. It now glorifies visibility over wisdom, often rewarding reach rather than substance. To avoid reinforcing this skewed digital culture, we have chosen to adopt the term "clickstar", capturing the reality that online fame today is often just a product of clicks, not credibility.

Our rising dependency on technology subtly reshapes our behaviours and expectations. Paying additional fees to avoid digital advertisements, a departure from traditional media consumption, demonstrates how immediacy fuels impatience. Such behavioural changes suggest broader implications covered in the Emerging Technologies chapter, cautioning that abandoning traditional norms could lead to significant financial costs merely to sustain conveniences previously enjoyed without additional expense.

In India, I have noticed a curious trend: accessing basic services seems contingent upon first providing a contact number, swiftly followed by the next

steps. These shifts demand an informed, rights-aware citizenry: consumers must recognise that so-called "free" conveniences and loyalty points are often *data-for-discount* trade-offs, where personal information underwrites the service. Before parting with phone numbers, identity proofs, or behavioural data, we must learn to read and question privacy notices and data-protection policies, exercising consent with intention rather than haste, an ethic [and an ecosystem] this book seeks to cultivate. Additionally, the rapid rise in UPI-based payments raises concerns around whether we have unintentionally gamified financial spending, potentially fostering impulsive behaviours. These intricate dynamics receive a detailed exploration in our chapters on the Information Technology Act, Cybercrimes, and Data Protection.

Privacy and Data Protection have become the defining fault lines of the digital age. In an ecosystem where personal information is constantly collected, analysed, and monetised, the individual's right to control their data is often overshadowed by the commercial and governance imperatives of those who hold it. Data breaches, unauthorised surveillance, and opaque consent mechanisms demonstrate how fragile privacy can be when left unguarded. At the same time, effective data protection frameworks are not only about shielding individuals from harm—they are also about fostering trust in digital transactions and innovation. As explored in the chapters on Privacy and Data Protection, the challenge lies in striking a balance: empowering individuals with control over their digital identities, while enabling businesses and governments to harness data responsibly and ethically. Without robust safeguards, the very transparency and efficiency that technology promises could erode into surveillance, manipulation, and mistrust.

Visibility driven by technology has altered who we trust and why. Increasingly, public trust is anchored in digital presence rather than genuine wisdom or expertise—a potentially risky trajectory for society. As we traverse this complex digital terrain, it is crucial to manage what *Ralph Gomory* in his taxonomy of knowledge called the known, unknown, and unknowable (KuU) risks, with methods and strategies comprehensively outlined in our Information Security chapter.

Finally, the advent of artificial intelligence raises critical questions regarding job markets—I think it will not go through outright job replacement, but rather by rendering certain skills and roles irrelevant. However, I am also hopeful that AI integration will assist in creating new roles, which may not be foreseeable today. This necessitates proactive policy frameworks and workforce adaptability, a concern thoroughly addressed in our Emerging Technologies and Data Protection chapters.

This book strongly advocates for a mindful, deliberate approach towards technology deployment and adoption. Equipped with insights on laws, regulatory frameworks, and digital policies, readers will be empowered to responsibly navigate—and actively shape—the continually evolving digital landscape. This book is not just a guide to understanding the digital landscape; it is an invitation to shape it thoughtfully, responsibly, and sustainably.

It is for the students and early-career professionals who want a rigorous yet readable map of the terrain; for practitioners and in-house counsels who need issue-spotting frameworks that travel well across industries; for Judges, regulators, and policymakers building the capacity to weigh technical evidence and set proportionate rules; for founders and product teams intent on turning compliance from an external constraint into an internal design principle; and for informed citizens who want to understand their rights, and the trade-offs tucked into default settings, loyalty programmes, and frictionless payments. If you build, buy, deploy, litigate, regulate, or simply live with technology, this book is for you.

I would conclude with a caution—technology law is a moving target. We have timestamped particularly fluid areas and, where useful, indicated competing approaches. Our commitment is to reasoning that ages better than a specific citation: if the facts change, the method should still guide you to a defensible answer. Ultimately, this field advances when communities compare notes. If you spot errors, disagree with our conclusions, or have examples that sharpen a doctrine, we hope you will treat this book as the beginning of a conversation rather than the end of one.

With all good wishes,

Nikhil Naren

LL.M. [United Kingdom] (2021-2022); B.A.LL.B. [India] (2015-2020)

Chevening Scholar

Assistant Director, Cyril Shroff Centre for AI, Law and Regulation; and Assistant Professor, Jindal Global Law School, Sonipat

Of Counsel, Scriboard [Advocates and Legal Consultants], New Delhi

Visiting Faculty, National Law University, Delhi

Visiting Faculty, West Bengal National University of Juridical Sciences, Kolkata

Visiting Faculty, National Law University, Odisha

Former Consultant, Digital Economy Capacity-Building Section, United Nations Conference on Trade and Development [UNCTAD], Geneva

CONTENTS

Chapter 2
Navigating the Shadowy Realms of Cybercrimes

Chapter 3

Evidence Unplugged: *Decoding the Digital Clues*

Chapter 4

The Future of Security

Chapter 5

Who's watching you? Understanding Surveillance

Chapter 6

Reclaiming Privacy in the Digital Age

Chapter 7

Digital Personal Data Protection Act, 2023 in a Global Perspective

Chapter 8

Open Mic or Muffled Voices? – Free Speech, Defamation, and Jurisdictional Challenges

Chapter 9

Demystifying E-governance

Chapter 10

From Clicks to Carts

Chapter 11

Like, Share, but be Aware

Chapter 12

Protecting Intellectual Property in the Digital Wilderness

Chapter 13

Branding Bytes – Mastering Digital Brand Management

Chapter 14

Privacy Policies – *Simplifying the Fine Print*

Chapter 15

Unlocking Tomorrow: *Exploring Emerging Technologies*