VIKHRAM S
Department of Computer Science and Engineering (Cyber Security) | Saveetha Engineering College

Cyber Law and Compliance Series: Security, Contracts, and Intellectual Property in the Digital Era

By Vikhram S, Advisor, Machine Learning Community – Tech Society, Saveetha Engineering College

Invited lecture delivered to the Department of Computer Science and Engineering (Cyber Security), Saveetha Engineering College, 2026

Every one of you already lives a large part of your life online – you sign up for services by clicking "I agree," you shop, you bank, and you share creative work over the internet without a second thought. Cyberspace, however, does not erase the legal questions that have always governed human transactions; it simply asks them in new forms. Today's lecture walks through three of those questions in turn: how do we form a binding agreement without paper and signatures; how do we secure data that never sits still; and how do we protect ideas and creative work once they can be copied infinitely, instantly, and anonymously. These three aspects – contracts, security, and intellectual property – together form the backbone of what we call cyber law.

1. The contract aspect of cyber law

Technology has quietly rewritten how agreements are made. What used to require two people in a room with a pen has become a click, a tap, or an exchange of emails. E-commerce has grown into one of the most profitable industries in the world precisely because the internet can act as an intermediary that carries an offer from one party and an acceptance from another, instantly, across any distance. In India, this shift is governed by a combination of three statutes working together: the Information Technology Act, 2000, which gives electronic records and signatures legal recognition; the Indian Contract Act, 1872, which supplies the underlying rules of what makes any agreement binding; and the Evidence Act, 1872, which determines how electronic records can be proven in court. The COVID-19 pandemic accelerated this shift further, pushing even courts toward virtual hearings and pushing business of every scale onto digital rails.

1.1 What is an e-contract?

An e-contract is simply an agreement formed electronically rather than through a physical meeting. It is a subset of the broader category of e-business, and it follows the same fundamental principles as any oral or written contract – there must be an offer, an acceptance, and an intention to be legally bound. What changes is the mechanism. Section 10 of the IT Act authorises contracts formed this way, and Section 2(p) of the same Act defines the electronic or digital signature that can stand in for a handwritten one. This matters most in high-stakes settings, such as government-to-government or government-to-business contracts, where a verifiable digital signature is essential. A useful illustration is the Supreme Court's reasoning in *Trimex International FZE Ltd. Dubai v. Vedanta Aluminium Ltd.*, where the Court held that a contract concluded entirely over email, without any physically signed document, was still valid once offer and acceptance had been clearly communicated.

1.2 Five ways an e-contract can be formed

The five recognised kinds of electronic contracts Graph 1

Shrink-Wrap	Click-Wrap	Browse-Wrap	Scroll-Wrap	Sign-In Wrap
Terms bind the buyer the moment software packaging is opened	User clicks “I Agree” before installing or accessing a service	Continued use of a website implies acceptance, with no active click	User must scroll through the full terms before assenting	Acceptance is bundled into the act of signing in or registering

Source: Author's synthesis, adapted for classroom presentation.

1.3 Where things get complicated: jurisdiction

Because e-contracts are paperless and inherently cross-border, one of the hardest practical questions they raise is jurisdiction – which court, in which state or country, has the authority to hear a dispute. The IT Act offers a starting rule: the originator's place of business is treated as the place from which information was dispatched, and the addressee's place of business is treated as where it was received. But this is not the whole story. Section 20 of the Code of Civil Procedure, 1908, allows a suit to be filed wherever the cause of action arises, which for an e-contract may be the place where an email was sent or received, regardless of either party's principal place of business. In *P.R. Transport Agency v. Union of India*, the Allahabad High Court held that because the acceptance of a contract was emailed to and received in Chandauli, Uttar Pradesh, that was where jurisdiction properly lay – even though the petitioner's principal place of business was elsewhere in the state. The broader lesson for students building or using digital platforms is that the absence of a signature and a physical meeting place does not remove legal accountability; it just shifts the proof of that accountability onto server logs, timestamps, and email records, which carry their own risk of loss through technical failure with no settled legal framework yet for who bears that loss.

2. The security aspect of cyber law

If contract law asks how an agreement is formed, security law asks a more defensive question: how do we keep the data behind that agreement safe from people who should never have touched it? Electronic data in transit is vulnerable to unauthorised interference in a way that a signed paper document locked in a filing cabinet never was, and the growth of e-commerce depends directly on how effective the surrounding legal and technical infrastructure is at closing that gap.

2.1 What organisations actually report

A useful reality check comes from Ernst & Young's Information Security Survey, which polled more than 4,300 IT managers across 29 countries. Its findings are a good antidote to the assumption that security is purely a technical problem solved once and forgotten.

What the Ernst & Young Information Security Survey found Graph 2

82%	50%+	80%	20%
of senior executives now rate information security as important, up sharply from five years earlier	of respondents are not confident their systems could withstand an internal attack	say winning top management's commitment is the single biggest key to improving security	of surveyed companies still had no formal security policy in place at all

Source: Ernst & Young, Information Security Survey 2000; author's synthesis for classroom presentation.

The survey also found that of the organisations that had already suffered a security breach in the previous year, only half had taken adequate steps to prevent a repeat. Among the weaknesses it uncovered: 36% of organisations did not monitor for network incidents at all, 53% did not monitor their own online activity including internet use, and 64% had no planned incident response process. Tellingly, when asked what stood in the way of improvement, respondents pointed less to a lack of management buy-in and more to a shortage of human resources and employee awareness – a reminder that security is as much a people problem as a technology one.

2.2 The basic technical safeguards

Underneath the policy layer sit a handful of technical mechanisms that most of you already use without necessarily naming them. Access control restricts a system to authorised users only, ranging from something as simple as physically locking a computer to requiring a password before any data can be viewed. A firewall protects a network from unauthorised external interference by filtering traffic at its boundary. Encryption protects data while it moves: specialised software scrambles information before it is transmitted, and only a computer holding the matching software can decode it, which insulates the data from interception along the way.

2.3 India's legal security framework

India's statutory backbone for cybersecurity has grown in layers. The Information Technology Act, 2000 remains foundational: it gives electronic records and signatures legal standing and sets out penalties for offences such as unauthorised access under Section 43 and hacking under Section 66. The IT Amendment Act, 2008 added more specific offences – identity theft under Section 66C, cheating by personation under Section 66D, and violation of privacy under Section 66E. More recently, the Digital Personal Data Protection Act, 2023 focused squarely on how digital personal data is processed, requiring consent and building in privacy safeguards. An anticipated Digital India Act is expected eventually to replace the original IT Act altogether, in recognition of how much the digital ecosystem has changed since 2000.

2.4 Institutions and regulatory focus areas

Legislation alone does not enforce itself; India has built institutions around it. CERT-In, the Indian Computer Emergency Response Team, is authorised under Section 70B of the IT Act as the national agency for incident response and vulnerability management, and organisations are required to report a data breach to CERT-In within six hours of noticing it – a strikingly short window that reflects how quickly a breach can spread. Separately, Critical Information Infrastructure, covering systems such as banking and defence whose compromise would cause national-level harm, receives its own dedicated protective guidelines, and intermediaries such as social media platforms and internet service

providers are required to exercise "due diligence" in removing illegal content under the IT Rules. On the enforcement side, Section 66F of the IT Act carries stringent penalties for acts of cyber terrorism intended to threaten the nation's unity, integrity, or security; separate provisions allow authorities to freeze accounts and trace digital transactions in cases of financial fraud; and companies handling sensitive personal data are legally required to implement what the law calls "reasonable security practices" to protect it.

3. The intellectual property aspect of cyber law

The third pillar of today's lecture concerns something less tangible than a contract or a firewall: ideas. Intellectual Property Rights, or IPR, are the legal rights granted to people who create original work – in art, literature, photography, writing, music, choreography, and audio or video – giving them exclusive control over how that work is used commercially. The internet has been enormously good for creators in one sense, giving them global reach at almost no cost, and enormously dangerous in another, because the same technology that distributes a creative work instantly also makes it trivially easy to copy, alter, and redistribute without permission.

3.1 Types of intellectual property, and India's legislative backbone

IPR is generally divided into patents, copyrights, trademarks, trade secrets, industrial and layout designs, and geographical indications. India built much of its modern IPR framework in a single legislative push in 1999, aligning domestic law with the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). That year saw the Patents (Amendment) Act, 1999, which introduced a mailbox system for filing patents and extended exclusive marketing rights; the Trademarks Bill, 1999; the Copyright (Amendment) Act, 1999; the Geographical Indications of Goods (Registration and Protection) Bill, 1999; the Industrial Designs Bill, 1999, which replaced the older Designs Act of 1911; and a further Patents (Second Amendment) Bill, 1999, bringing the 1970 Patents Act fully into compliance with TRIPS.

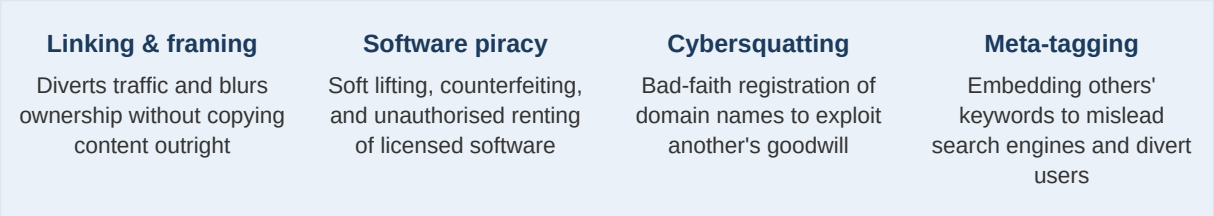
3.2 Recurring challenges online

Four categories of dispute come up again and again in practice. The first is copyright infringement in its various online-specific forms. **Linking** directs a user to another page without leaving the current one, which can quietly divert traffic and revenue away from the original site and create a false impression that the two sites are affiliated. **Deep linking** compounds the problem because it is genuinely unclear, under Sections 14 and 51 of the Copyright Act, 1957, at exactly what stage an infringement occurs – when the link is created, or only when a user actually clicks it. **In-linking** lets a page silently pull in images from other websites, so that the final viewer has no idea the content originated elsewhere, and **framing** raises the unresolved question of whether combining someone else's content inside your own page counts as a new, adapted work or simply unauthorised reproduction.

The second category is software piracy, which takes several forms: soft lifting, sharing licensed software with someone who has no license of their own; counterfeiting, producing fake copies complete with imitation packaging and manuals; and unauthorised renting of software in violation of its license terms. The third is cybersquatting and trademark infringement – registering a domain name that imitates a famous one in order to profit from its goodwill or confuse its users, which becomes especially contentious when two parties both claim a right to the same name. A domain name is

generally treated as abusive when it mimics a registered trademark, misleads users into visiting it by mistake, was registered without any legitimate right or interest, and is being used in bad faith. The fourth is meta-tagging, quietly embedding a competitor's keywords into a site's metadata so that search engines misdirect traffic toward it, which can itself amount to trademark infringement.

Four recurring categories of online IP disputes Graph 3



Source: Author's synthesis, adapted for classroom presentation.

3.3 Jurisdiction, and how Indian law responds

Cyberspace has no borders, which makes IP disputes a genuinely global concern; deciding which court has authority to hear a case – the question of jurisdiction – remains one of the least settled areas of the field. Indian law provides several statutory anchors nonetheless. Section 51 of the Copyright Act, 1957 vests exclusive rights in the copyright owner and treats anything contrary to those rights as infringement; because no dedicated legislation fixes the liability of internet service providers, courts have read Section 51 to require both knowledge and a lack of due diligence before an ISP can be held liable. Section 79 of the IT Act, 2000 offers intermediaries a conditional safe harbour from liability for third-party content, subject to the due-diligence obligations set out in the 2021 Intermediary Guidelines. On cross-border reach, Section 75 of the IT Act extends India's jurisdiction to any cybercrime committed outside the country if it targets a computer, computer system, or computer network located in India, and Section 4 of the Indian Penal Code, 1860 similarly extends to offences committed abroad that target a computer resource located in India. Together, these provisions let Indian courts protect intellectual property owners even when the infringing act technically originates outside the country.

Closing note

The three threads in today's lecture – contracts, security, and intellectual property – are really one story told from three angles: how cyberspace lets us form relationships, how we protect what flows through those relationships, and how we protect what we create within them. My advice to you as future engineers and technologists is to treat this not as a subject you study once for an exam, but as a lens you carry into every system you ever build: who is agreeing to what, what happens to their data, and whose original work you might be touching.

For queries, project proposals, ideas, or guidance related to this lecture, please write to vikhrams@saveetha.ac.in.