DegreeLive

BBA | Semester I | UK1DSCMGT103

E-Commerce and Cyber Law

Course Code: UK1DSCMGT103 • Module 3 Notes

Module III: Cyber Law Frameworks and Intellectual Property Rights

1. Concept, Genesis, and Jurisdictional Challenges of Cyber Law

The emergence of the digital network environment created an unprecedented socio-economic domain termed *Cyberspace*. Coined conceptually by science fiction author William Gibson in 1984, cyberspace represents the global, virtual, intangible realm of interconnected electronic devices, telecommunications backbones, software platforms, and digital data flows. Unlike the physical territorial world divided by sovereign geographic borders, rivers, and national walls, cyberspace is inherently decentralized, borderless, instantaneous, and non-physical.

Traditional legal jurisprudence evolved over centuries on the doctrine of **Territorial Sovereignty**—the sovereign authority of a nation-state to enact and enforce binding laws over people, physical property, and transactions situated strictly within its demarcated territorial boundaries. When commercial transactions and criminal offenses shifted to computer networks, this territorial framework broke down. A consumer situated in Kochi can purchase software hosted on a cloud server in Ireland, processed through an acquiring bank in Singapore, using an application designed in California. If a dispute or financial breach occurs, which legal forum possesses judicial authority? This profound jurisdictional dilemma necessitated the birth of **Cyber Law**.

Key Jurisdictional Complexities in Cyberspace

Cyber law is the comprehensive legal discipline encompassing statutory enactments, administrative regulations, judicial doctrines, and international treaties that govern the Internet, digital communications, electronic commerce, information security, and computer-related activities. Key challenges include:

- **The Extraterritorial Jurisdiction Dilemma:** Determining whether a domestic national court has the legal authority to adjudicate cases involving foreign defendants whose electronic actions cause harmful economic or personal impacts within the domestic forum. In private international law, courts apply evolving tests such as the *Effects Doctrine* (exercising jurisdiction if foreign actions produce direct, substantial, and foreseeable effects within the territory) and the *Zippo Sliding Scale Test* (evaluating website interactivity, from passive informational sites to active transactional web portals).
- **Choice of Law and Choice of Forum:** In cross-border e-commerce disputes, resolving which jurisdiction's substantive laws govern the contract and which nation's courts possess the legitimate authority to adjudicate claims. E-commerce platforms address this through mandatory standard-form click-wrap dispute resolution and forum-selection clauses.
- **Anonymity and Attribution:** The decentralized architecture of internet packet routing, combined with Virtual Private Networks (VPNs), proxy servers, encrypted darknets (Tor), and spoofed IP headers, makes tracing the true physical identity of online wrongdoers exceptionally difficult.

2. Global Harmonization: The UNCITRAL Model Laws

To prevent a chaotic patchwork of conflicting national internet regulations from paralyzing international e-commerce, the United Nations Commission on International Trade Law (UNCITRAL) formulated foundational international legal models:

A. UNCITRAL Model Law on Electronic Commerce (1996)

Adopted by the United Nations General Assembly in resolution 51/162, the Model Law provided universal legislative templates for national parliaments to modernize domestic commercial codes. The Model Law is founded upon two revolutionary legal principles:

- **Principle of Non-Discrimination:** Codified in Article 5, establishing that information shall not be denied legal effect, validity, or enforceability solely on the grounds that it is in the form of a data message.
- **Principle of Functional Equivalence:** Rather than forcing digital technology to mimic physical paper procedures, the Model Law analyzed the fundamental legal functions fulfilled by traditional paper documents (e.g., providing an evidentiary record, signifying personal assent via handwritten signature, proving original authenticity) and established criteria under which electronic records fulfill those identical legal functions.

B. UNCITRAL Model Law on Electronic Signatures (2001)

Expanded digital signature frameworks by establishing standards of technological neutrality, presumption of signer intent, and operational duties of relying parties and certification service providers. The UNCITRAL Model Laws served as the direct legislative blueprints for national statutes worldwide, including India's **Information Technology Act, 2000**.

3. Public Policy Dimensions, Consumer Protection, and Data Sovereignty

E-commerce operates at the intersection of private commercial contracts and public policy governance. Governments must balance fostering digital innovation with protecting vulnerable consumers from fraud, algorithmic exploitation, and cross-border digital harms.

A. Consumer Protection in Digital Transactions

In India, digital consumers were historically vulnerable to unfair trade practices, hidden pricing, counterfeit goods, and refused returns under traditional physical sales laws. To bridge this gap, India enacted the **Consumer Protection Act, 2019** and promulgated the specialized **Consumer Protection (E-Commerce) Rules, 2020**. Key statutory protections include:

- **Mandatory Entity Transparency:** Every e-commerce entity must prominently display its legal corporate name, registered address, website, customer care contact details, and ticket generation mechanisms on its digital platforms.
- **Prohibition of Unfair Trade Practices:** Platforms are strictly prohibited from manipulating search algorithms to favor in-house or affiliated sellers, displaying misleading pricing, adopting deceptive dark patterns, or posting fabricated, incentivized consumer reviews.

Degree Live

- **Clear Disclosure of Country of Origin:** Sellers must disclose the physical country of origin for all listed goods, enabling informed consumer choice.
- **Statutory Grievance Redressal Mechanism:** E-commerce entities must appoint a dedicated resident Grievance Officer, acknowledge consumer complaints within 48 hours, and resolve grievances within one month.

B. Cross-Border Data Flows and Data Sovereignty

Data has become the primary economic asset of modern digital capitalism. Multinational technology conglomerates routinely harvest massive volumes of personal data from developing nations, transferring and storing it in foreign server farms for AI training and commercial monetization. This extraction generated intense debates over **Data Sovereignty**—the sovereign right of a nation-state to govern and regulate digital data generated by its citizens within its territorial jurisdiction.

Nations balance two competing policy paradigms: (1) *Free Cross-Border Data Flows:* Championed by multinational corporations to preserve seamless cloud interoperability and global digital trade; and (2) *Data Localization Mandates:* Statutory requirements forcing corporations to store critical personal, financial, and biometric data on servers physically located within national borders (e.g., the Reserve Bank of India's 2018 directive mandating that all payment system data must be stored exclusively on systems located in India).

4. Privacy Rights, Personally Identifiable Information (PII), and Cookie Governance

In modern information societies, digital privacy is recognized as a fundamental human right. In the historic nine-judge constitutional bench ruling in **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)**, the Supreme Court of India unanimously declared that the **Right to Privacy is a Fundamental Right** protected under Article 21 and Part III of the Constitution. Privacy encompasses informational privacy—the right of an individual to control the dissemination and commercial exploitation of their personal data.

A. Personally Identifiable Information (PII) and Data Protection Architecture

Personally Identifiable Information (PII) represents any information that can be used directly or indirectly to distinguish, identify, or trace an individual's personal identity (name, Aadhaar number, passport details, phone number, biometric fingerprints, geolocation, financial banking records, medical histories). To safeguard PII, modern legal frameworks—such as the European Union's **General Data Protection Regulation (GDPR)** and India's **Digital Personal Data Protection Act, 2023 (DPDP Act)**—enforce foundational data protection principles:

- **Consent and Purpose Limitation:** Personal data can be collected and processed strictly with the explicit, informed, unambiguous, and revocable consent of the data principal for lawful, specific, clearly stated purposes.
- **Data Minimization:** Organizations must collect only the minimum quantum of personal data strictly necessary to fulfill the stated operational purpose.

- **Storage Limitation:** Personal data must not be retained longer than necessary to satisfy the business purpose for which it was originally collected.
- **Data Security Safeguards:** Entities (Data Fiduciaries) must deploy reasonable technical and organizational security measures (encryption, pseudonymization, access controls) to prevent unauthorized access or data breaches.
- **Rights of Data Principals:** Individuals possess statutory rights to access summaries of their processed data, demand correction of inaccurate records, request complete erasure of personal data, and nominate representatives.

B. Cookie Governance and Tracking Technologies

HTTP cookies are small text files placed on a user's web browser by web servers to log session states, remember shopping carts, and track browsing patterns. Privacy regulations distinguish between: (1) *Strictly Necessary Session Cookies:* Essential for basic site security and shopping cart functionality, exempt from prior consent; (2) *Persistent Third-Party Tracking Cookies:* Deployed by advertising networks across multiple websites to construct behavioral psychographic consumer profiles for targeted ad auctions. International privacy laws mandate explicit, upfront cookie consent banners, prohibiting pre-ticked consent boxes and giving users transparent rights to reject tracking.

5. Intellectual Property Rights (IPR) in Cyberspace

Intellectual Property Rights represent legal monopoly rights granted to creators over intangible creations of the human mind. The ease with which digital files can be copied perfectly, distributed instantaneously, and modified without degradation creates severe challenges for traditional IPR frameworks.

A. Digital Copyright and Software Protection

Copyright protects original literary, dramatic, musical, and artistic works. In cyber law, computer software programs and source code are legally protected as "literary works" under the Indian Copyright Act, 1957 and the WIPO Copyright Treaty (WCT 1996):

- **The Idea-Expression Dichotomy:** Copyright protects the specific creative expression of an idea, not the underlying idea, algorithm, or mathematical concept itself. Two software applications can achieve identical functional outcomes, but if their underlying source code is independently written without copying, no infringement occurs.
- **Software Licensing Models:** Proprietary Commercial Licenses (granting restricted, non-exclusive rights to run compiled binary code while keeping source code secret under End User License Agreements - EULAs) versus Free and Open-Source Software (FOSS) licenses (such as GNU General Public License - GPL, MIT, Apache) that grant users legal freedom to inspect, modify, and redistribute source code.
- **Digital Rights Management (DRM) and Technological Protection Measures (TPM):** Hardware and software encryption locks embedded into digital media to prevent unauthorized copying. Circumventing technological protection measures or altering digital rights management metadata is a statutory criminal offense under Section 65A and 65B of the Indian Copyright Act.

B. Online Trademark Infringement and Keyword Bidding

A trademark is a distinctive visual sign, word, logo, or symbol that identifies goods and services as originating from a specific commercial enterprise, protecting consumer goodwill and preventing marketplace confusion. In cyberspace, trademark conflicts manifest through:

- **Metatags and Invisible Keyword Stuffing:** Unscrupulous website developers embed competitor registered trademarks into their HTML hidden metadata, search tags, or white-on-white text to deceive search engine spiders into indexing their site for competitor search queries. Courts classify this as trademark infringement and passing off.
- **Search Engine Keyword Bidding (Google AdWords Disputes):** Competitors bidding on registered trademarks as advertising trigger keywords. In landmark rulings, courts held that using a competitor's trademark to trigger sponsored search ads does not constitute infringement provided the resulting advertisement text does not cause consumer confusion regarding product origin or falsely imply affiliation.
- **Deep Hyperlinking and Framing:** Bypassing a website's homepage, terms of service, and advertising banners to link directly to deep internal content (deep linking), or embedding a third-party website's pages within an inline HTML frame under one's own domain banner, deceiving users regarding content origin.

6. Domain Name Disputes: Cybersquatting, Typosquatting, and ICANN UDRP

The Domain Name System (DNS) was originally designed as a technical addressing scheme to translate numerical IP addresses into memorable textual strings. However, as e-commerce exploded, domain names evolved into invaluable global corporate business identifiers, rivaling traditional trademarks.

A. Taxonomy of Domain Name Piracy

- **Cybersquatting:** The bad-faith, intentional registration, trafficking in, or using of an Internet domain name that is identical or confusingly similar to a pre-existing famous trademark, with the bad-faith intent to profit by selling the domain back to the legitimate trademark owner at an exorbitant price, or diverting prospective customers to competitor services.
- **Typosquatting (URL Hijacking):** Registering common typographical errors, misspellings, or phonetic variations of popular brand domains (e.g., registering *goolge.com* or *amazn.com*). Typosquatters exploit keyboard mistyping to serve malware, phishing forms, or display aggressive advertising networks to unsuspecting consumers.

B. ICANN and the Uniform Domain Name Dispute Resolution Policy (UDRP)

The Internet Corporation for Assigned Names and Numbers (ICANN)—the non-profit organization coordinating global DNS root servers—established the **Uniform Domain Name Dispute Resolution Policy (UDRP)** in 1999 to provide a rapid, cost-effective administrative alternative to costly international court litigation. Under UDRP administrative proceedings (administered by accredited dispute resolution bodies like the World Intellectual Property Organization - WIPO

Arbitration and Mediation Center in Geneva), a trademark owner can secure the cancellation or transfer of a disputed generic top-level domain (.com, .org, .net) by proving three cumulative elements:

1. The disputed domain name is **identical or confusingly similar** to a trademark or service mark in which the complainant possesses legal rights; and
2. The domain registrant possesses **no rights or legitimate interests** in respect of the domain name (they are not commonly known by that name and make no bona fide non-commercial fair use); and
3. The domain name was **registered and is being used in bad faith** (e.g., registered primarily to sell to the brand owner for valuable consideration exceeding out-of-pocket costs, or registered to intentionally attract internet users for commercial gain by creating likelihood of confusion).

In India, disputes involving the country-code top-level domain (.IN) are adjudicated under the **.IN Dispute Resolution Policy (INDRP)** administered by the National Internet Exchange of India (NIXI).

7. Comprehensive Taxonomy of Cyber Threats and Attack Vectors

Managing an e-business requires a thorough technical comprehension of the diverse malicious software, social engineering methods, and network attack vectors deployed by cyber criminals:

Threat Category	Operational Mechanics and Payload	Organizational Impact and Defense
Malware and Computer Viruses	Malicious software programs designed to infiltrate computer systems without user consent. A traditional *Virus* attaches to legitimate executable host files and replicates when executed. A *Worm* is a standalone self-replicating program that exploits network vulnerabilities to spread automatically across networks without human intervention.	System corruption, data deletion, processor degradation. Mitigated via patched operating systems and Endpoint Detection and Response (EDR) software.
Trojan Horses and Spyware	A *Trojan Horse* masquerades as useful, benign software (a free game, utility tool) but conceals a hidden malicious backdoor payload. *Spyware* and Keyloggers secretly monitor user keystrokes, capturing banking passwords, credit card credentials, and business communications.	Credential harvesting, identity theft, unauthorized remote system control. Mitigated via application whitelisting and virtual sandboxes.
Ransomware	Advanced cryptographic malware that silently encrypts critical corporate files, databases, and system backups using high-grade asymmetric ciphers (RSA-4096, AES-256). Attackers display ransom notes demanding millions in untraceable cryptocurrency (Bitcoin, Monero) for decryption keys.	Paralyzes enterprise operations (e.g., WannaCry, NotPetya). Mitigated via immutable offline air-gapped backups and zero-trust network access.

Threat Category	Operational Mechanics and Payload	Organizational Impact and Defense
Phishing and Social Engineering	Manipulating human cognitive trust rather than exploiting software vulnerabilities. Attackers send fraudulent emails, SMS messages (Smishing), or voice calls (Vishing) that mimic trusted institutions (banks, tax authorities), tricking victims into divulging passwords or OTPs. *Spear-Phishing* targets specific high-value corporate executives (CEO Fraud / Whaling).	Account takeover, fraudulent corporate wire transfers. Mitigated via DMARC email authentication, hardware security keys, and employee training.
Denial of Service (DoS & DDoS)	Overwhelming an e-commerce server, network pipe, or API gateway with a massive flood of illegitimate traffic, exhausting CPU cycles, RAM, or bandwidth, rendering services unavailable to legitimate customers. Distributed DoS (DDoS) leverages global networks of millions of compromised, infected IoT devices (Botnets).	E-commerce downtime, millions in lost sales during peak events. Mitigated via cloud DDoS scrubbers (Cloudflare, AWS Shield) and rate-limiting.
Man-in-the-Middle (MITM) and Session Hijacking	An attacker intercepts communications between two legitimate parties (e.g., customer browser and banking portal) over unencrypted Wi-Fi or compromised routers, secretly reading or altering messages in real time.	Financial theft, unauthorized session takeover. Mitigated via mandatory HTTPS with HSTS and TLS 1.3 cryptographic protocols.

In conclusion, cyber law frameworks and intellectual property rights represent the indispensable legal guardrails of the digital economy. By harmonizing global procedural rules via UNCITRAL, enforcing robust data protection statutes, resolving international domain disputes through administrative arbitration, and fortifying defenses against sophisticated cyber threats, modern e-businesses construct the institutional trust required for global digital commerce.

8. Digital Watermarking, Steganography, and Multimedia Copyright Protection

To detect and legally prove intellectual property theft in cyberspace, content creators deploy advanced digital data-hiding technologies:

- **Digital Watermarking:** Embedding an indelible, permanent digital signal or signature directly into the underlying bitstream of a digital audio, video, image, or text file. Watermarks are categorized as: (1) *Visible Watermarks:* Semi-transparent corporate logos or copyright notices superimposed over images to deter unauthorized use; (2) *Invisible Robust Watermarks:* Cryptographically embedded into high-frequency spatial or Discrete Cosine Transform (DCT) coefficients. The watermark remains imperceptible to human senses, survives compression, cropping, and filtering, and can be extracted using forensic keys to prove copyright ownership in court.

- **Steganography:** The ancient art of concealing secret messages within ordinary, non-secret digital carriers (such as hiding an encrypted text file inside the least significant bits - LSB of a JPEG image file). Unlike cryptography (which conceals message meaning but advertises the existence of secret code), steganography conceals the very existence of the communication.

9. Advanced Cyber Threats: Zero-Day Exploits and Advanced Persistent Threats (APTs)

Modern cyber warfare has transcended amateur script kiddies, becoming dominated by sophisticated state-sponsored military intelligence units and organized cyber syndicates:

- **Zero-Day Vulnerabilities and Exploits:** A security flaw or software bug in an operating system, browser, or enterprise application that is completely unknown to the software vendor and lacks an existing security patch. Cyber criminals develop *Zero-Day Exploits* to attack targets before developers can issue defenses. On the dark web, zero-day vulnerabilities in mobile operating systems trade for millions of dollars.
- **Advanced Persistent Threats (APTs):** Highly covert, continuous, multi-stage cyber attacks conducted by well-funded state-sponsored threat groups (e.g., APT28, Lazarus Group). Rather than launching noisy defacements, an APT infiltrates an enterprise network silently, establishes persistent rootkit backdoors, moves laterally for months, and exfiltrates strategic intellectual property, commercial bids, and defense secrets without triggering basic alarms.
- **Supply Chain Attacks (Dependency Poisoning):** Infiltrating software developers or third-party open-source libraries rather than attacking the ultimate target directly. The catastrophic 2020 *SolarWinds Attack* infected legitimate software update patches, compromising thousands of government agencies and Fortune 500 corporations globally.

10. Digital Services Taxes, Equalisation Levy, and the OECD Global Tax Framework

Traditional international corporate taxation was built on the doctrine of **Permanent Establishment (PE)**: a multinational corporation was subject to corporate income tax in a sovereign jurisdiction strictly if it maintained a physical branch, office, factory, or physical agents within that nation's territorial borders. However, global digital technology monopolies (Google, Meta, Amazon, Netflix) generate billions of dollars in revenue from developing countries without establishing any physical corporate presence, booking digital revenues in low-tax offshore tax havens (such as Ireland, Bermuda, or the Cayman Islands).

To capture fair sovereign revenue, India became a global pioneer in digital taxation by enacting the **Equalisation Levy** (informally termed the "Google Tax"):

- **Equalisation Levy of 2016 (6%):** Imposed a direct statutory 6% tax on gross payments exceeding INR 1 Lakh made by Indian business residents to non-resident technology corporations for online digital advertising services.
- **Expanded Equalisation Levy of 2020 (2%):** Extended a 2% tax on the gross consideration received by non-resident e-commerce operators from e-commerce supply of goods or services

provided to Indian residents.

- **OECD Base Erosion and Profit Shifting (BEPS) Two-Pillar Solution:** Under the G20/OECD inclusive framework, over 135 nations agreed to a historic overhaul of international tax rules: (1) *Pillar One:* Reallocates 25% of residual profits of the largest multinational enterprises to market jurisdictions where consumers are physically located, regardless of physical presence; (2) *Pillar Two:* Establishes a mandatory **Global Minimum Corporate Tax Rate of 15%**, eliminating the incentive for digital corporations to divert profits to offshore tax havens.

11. Patentability of Computer Software in India: Section 3(k) Jurisprudence

In intellectual property law, the legal protection of software algorithms sits at the controversial boundary between copyright and patent law. Under **Section 3(k) of the Indian Patents Act, 1970**, the statute explicitly declares that *"a mathematical or business method or a computer programme per se or algorithms"* are strictly **NON-PATENTABLE INVENTIONS**.

The legislative phrase *"computer programme per se"* generated intense corporate litigation. The Delhi High Court in landmark rulings (e.g., *Ferid Allani v. Union of India, 2019*) clarified that the legislative intent was not to impose a blanket ban on all software inventions. If a computer-implemented invention demonstrates a **technical contribution** or produces a tangible **technical effect** beyond the normal physical interaction between program and hardware (e.g., software that optimizes digital image compression hardware, controls an industrial robotic arm, or manages a medical cardiac sensor), the invention is patentable. Pure abstract business methods or financial algorithms remain strictly unpatentable.

12. Judicial Precedents in Indian Domain Name Jurisprudence

Prior to the enactment of the IT Act, Indian courts faced complex domain name dispute litigation, resolving cases by applying traditional common-law doctrines of **Passing Off**. In landmark judicial rulings, the judiciary established that an Internet domain name is not a mere technical machine address, but a valuable corporate business identifier entitled to absolute legal protection:

- **Rediff Communication Ltd. v. Cyberbooth (2000):** The defendant registered the domain name *radiff.com* to operate an online portal mimicking *rediff.com*. The Bombay High Court held that the domain name was phonetically, visually, and deceptively similar, intended to mislead internet users, and granted an injunction restraining the defendant from using the mark.
- **Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd. (2004):** The Supreme Court of India delivered a watershed judgment on cybersquatting. The defendant registered *sifynet.com* and *sify.net*, encroaching upon the complainant's established trademark "Sify". The Supreme Court declared that: (1) Domain names have all the characteristics of trademarks and are entitled to equal statutory and common-law protection; (2) The primary purpose of a domain name is to identify a business and provide consumer recognition; (3) Injunctions must be granted against typosquatters to protect the consuming public from deception and confusion in cyberspace.

13. Consumer Protection (E-Commerce) Rules, 2020 in Detail

The specialized Consumer Protection (E-Commerce) Rules, 2020 enacted under the Consumer Protection Act, 2019 establish strict legal obligations on both marketplace platforms and inventory-led e-commerce entities:

- **Prohibition of Unreasonable Price Manipulation:** E-commerce entities are explicitly barred from manipulating the prices of goods or services offered on their platforms to gain unreasonable profits, discriminating between consumers of the same class, or arbitrarily creating artificial shortages.
- **Fall-Back Liability on Marketplace Platforms:** Historically, marketplace aggregators (Amazon, Flipkart) claimed they were neutral intermediaries with zero responsibility if a third-party seller sold defective or counterfeit goods. The statutory rules introduced *Fall-Back Liability*: if a third-party seller on a marketplace fails to deliver goods or services ordered by a consumer, or delivers counterfeit or defective goods, the marketplace platform incurs direct joint liability to refund and compensate the aggrieved consumer.
- **Regulation of Flash Sales:** While normal seasonal discount promotions are permitted, the rules prohibit "predatory flash sales" organized by platforms that limit consumer choice through exclusivity agreements with preferred affiliated sellers, ensuring a competitive, level playing field for traditional small retail merchants.

14. Deepfakes, Synthetic Media, and Generative AI Governance

The rapid proliferation of deep generative adversarial networks (GANs) and diffusion models has introduced the grave societal challenge of **Deepfakes**—hyper-realistic synthetic audio, video, and imagery that digitally clone a real person's voice, face, and mannerisms without their consent. Deepfakes are deployed for financial CEO fraud, non-consensual image abuse, and political disinformation:

- **Statutory Liability Under Indian Cyber Law:** Deepfakes trigger immediate criminal prosecution under multiple sections of the IT Act: Section 66D (Cheating by personation using a computer resource), Section 66E (Violation of bodily privacy), Section 67 / 67A (Transmitting sexually explicit content), and Sections 499 and 500 of the Indian Penal Code (Criminal Defamation).
- **Intermediary Due Diligence Mandates:** Under the Intermediary Guidelines Rules, social media platforms are legally required to remove deepfake content within 24 to 36 hours upon receiving notice, deploy automated algorithmic detection tools, and mandatorily label AI-generated synthetic media with permanent cryptographic digital metadata watermarks.

15. Reverse Domain Hijacking (RDH) in Cyber Arbitration

Under the ICANN UDRP framework, domain arbitration mechanisms must prevent wealthy multinational corporations from abusing administrative procedures to bully legitimate small domain owners. **Reverse Domain Name Hijacking (RDH)** is formally defined as the bad-faith attempt by a trademark owner to harass, coerce, or deprive a registered domain-name holder of a legitimate

domain name through baseless UDRP complaints. If a WIPO arbitration panel finds that the trademark complainant knew or should have known that the domain owner possessed legitimate non-commercial rights or registered the domain prior to the trademark's creation, the panel issues a formal finding of Reverse Domain Hijacking, condemning the complainant's bad-faith procedural abuse.

DegreeLive