THE LAWWAY WITH LAWYERS JOURNAL
Website: www.the lawway with lawyers.com
VOLUME:-36 ISSUE NO:- 36 , JUNE 19, 2026
ISSN (ONLINE):- 2584-1106
Email: thelawwaywithelawyers@gmail.com
Digital Number : 2025-23534643
CC BY-NC-SA
Authored By :- Aafiah Hasnain
Amity University, Patna

THE DARK WEB AND COPYRIGHT INFRINGEMENT: LEGAL CHALLENGES

Abstract

The rapid growth of the internet has transformed the way digital content is created, accessed, shared, and distributed. Alongside these developments, the Dark Web has emerged as a relatively anonymous and difficult-to-regulate part of the internet, creating new challenges for the protection and enforcement of copyright. The unauthorized copying, sharing, selling, and distribution of copyrighted materials such as films, music, books, software, photographs, and other digital content can cause significant harm to copyright owners and content creators. The anonymity and decentralized nature associated with the Dark Web may make it more difficult to identify infringers, trace the source of unauthorized content, establish jurisdiction, and effectively enforce existing copyright laws. This research paper seeks to examine the relationship between the Dark Web and copyright infringement, with particular attention to digital piracy and the unauthorized use and distribution of online content without the permission of copyright holders. It will analyse whether existing copyright laws are sufficiently equipped to address infringement occurring through anonymous and technologically complex online environments. The paper will also examine issues relating to intermediary liability, jurisdiction, anonymity, evidence collection, website blocking, and the practical difficulties faced by law-enforcement agencies and copyright owners. In the Indian context, the study will consider the relevant provisions of the Copyright Act, 1957, along with developments in Indian judicial practice concerning online piracy and digital copyright enforcement. The research ultimately aims to identify the gaps between existing legal mechanisms and the technological realities of the Dark Web and to suggest possible approaches for strengthening copyright protection while maintaining a balance with legitimate uses of digital content and individual rights.

Keywords: Dark Web, Copyright Infringement, Digital Piracy, Online Enforcement, Intermediary Liability, Anonymity, Jurisdiction, Website Blocking, India, Cyber Law.

Introduction

The development of digital technology has fundamentally changed the nature of copyright. Copyright was historically designed around comparatively identifiable acts of reproduction, publication, distribution and communication. Digital technology, however, has made the reproduction and distribution of creative works extremely rapid, inexpensive and geographically unrestricted. A single digital copy of a film, book, song, photograph or computer programme can potentially be reproduced and distributed to thousands of users without any physical degradation of the original. The internet has therefore expanded both the economic opportunities available to copyright owners and the possibilities for large-scale infringement.

The emergence of the Dark Web adds another layer of complexity to this problem. The term "Dark Web" generally refers to online content accessible through specialised networks and software that are designed to provide a higher degree of anonymity than the ordinary or "surface" web. The Dark Web should not be confused with the Deep Web. The Deep Web includes content that is not indexed by ordinary search engines, such as private databases, institutional portals and password-protected services, whereas the Dark Web refers to services deliberately operating through anonymity-oriented networks. The Tor network is the most prominent example. According to the United Nations Office on Drugs and Crime (UNODC), Dark Web services operate through specialised encrypted networks and are designed to make the identification and tracking of users and services more difficult.[1]

Anonymity itself is not unlawful. Privacy-enhancing technologies may serve legitimate purposes, including protecting journalists, whistle-blowers, human-rights defenders and individuals living under repressive regimes. The legal problem arises when the same technological characteristics are used to facilitate unlawful conduct. Copyright infringement may occur where copyrighted works are copied, uploaded, stored, offered for sale, distributed, streamed or otherwise communicated to the public without authorisation. Dark Web environments can therefore become an additional venue for digital piracy.[1]

The principal legal difficulty is not necessarily that copyright law fails to recognise the underlying conduct. Reproducing or distributing a copyrighted work without permission may constitute infringement regardless of whether the act occurs on the surface web, a private

[1] United Nations Office on Drugs and Crime, *Darknet Cybercrime Threats to Southeast Asia* (UNODC 2021) 7–10. The report explains that the Dark Web operates through specialised encrypted networks, particularly Tor and I2P, designed to conceal user and server identities.

network or a Dark Web service. Rather, the central difficulty lies in **identifying the infringer, locating the relevant infrastructure, preserving evidence, establishing jurisdiction, obtaining information from intermediaries, and enforcing judicial orders across borders**.

The World Intellectual Property Organization (WIPO) has recognised that digital technology has created significant challenges for the copyright system because works can be distributed globally and rapidly through digital networks. The WIPO Copyright Treaty (WCT), adopted in 1996, specifically addresses copyright protection in the digital environment and supplements the Berne Convention by recognising, among other things, a broader right of communication to the public.[2]

The Indian legal framework contains several provisions capable of addressing online copyright infringement. The Copyright Act, 1957 provides the principal statutory framework, while the Information Technology Act, 2000 regulates several aspects of digital activity and intermediary liability. Sections 51 and 55 of the Copyright Act are particularly relevant to infringement and civil remedies, while section 63 creates criminal liability for knowing infringement. Sections 65A and 65B additionally address technological protection measures and rights-management information.[3]

The question, therefore, is not simply whether copyright infringement on the Dark Web is illegal. The more significant question is whether conventional mechanisms of copyright enforcement are sufficiently effective when the identity, location and technological infrastructure of the infringer may be deliberately concealed.

2. Research Objectives

This research has five principal objectives. First, it seeks to explain the relationship between the Dark Web and digital copyright infringement. Secondly, it examines the major legal and technological difficulties involved in identifying and prosecuting Dark Web infringers. Thirdly, it analyses the adequacy of Indian copyright and information-technology law in addressing such infringement. Fourthly, it evaluates judicial mechanisms such as intermediary

[2] World Intellectual Property Organization, *Copyright in the Digital Environment*; WIPO Copyright Treaty (adopted 20 December 1996). WIPO describes the WCT as a special agreement under the Berne Convention addressing copyright protection in the digital environment.

[3] The Copyright Act 1957, ss 51, 55, 63, 65A and 65B. See also Copyright Office, Government of India, *The Copyright Act, 1957*. The current statutory text confirms the provisions relating to technological measures and rights-management information.

liability, website blocking and dynamic injunctions. Finally, it proposes legal and institutional approaches capable of improving enforcement while protecting legitimate interests in privacy, freedom of expression, research and access to information.

3. Research Methodology

The paper adopts a **doctrinal and analytical legal research methodology**. Primary sources include the Copyright Act, 1957, the Information Technology Act, 2000, relevant rules, international copyright instruments and judicial decisions of Indian courts. Secondary sources include academic articles, books, institutional reports and publications of organisations such as WIPO and UNODC.

The research is principally qualitative rather than empirical. It does not attempt to calculate the total volume of copyright infringement occurring on the Dark Web. This limitation is important because the anonymous character of Dark Web networks makes reliable measurement difficult. Instead, the paper examines the legal consequences of anonymity, decentralisation, transnational infrastructure and technological concealment.

4. Understanding the Dark Web and Its Relationship with Copyright Infringement

The internet is often described through three broad categories: the Surface Web, the Deep Web and the Dark Web. The Surface Web consists of websites indexed by conventional search engines. The Deep Web consists of online material that is not ordinarily indexed, including private accounts and databases. The Dark Web represents a much smaller portion of online activity and is intentionally accessible through specialised anonymity networks.

Tor is particularly significant because it uses layered routing mechanisms to obscure the origin of internet traffic. Dark Web services can also conceal the physical location of servers through onion services. Consequently, the ordinary relationship between a website, a domain name, an IP address and a physical server may become considerably more complicated.

This technological architecture has legitimate purposes. Privacy-enhancing networks may protect vulnerable persons from surveillance, enable confidential communication and facilitate access to information. Therefore, it would be legally and conceptually incorrect to equate the

Dark Web itself with criminality. UNODC similarly observes that dark-net technologies are used for both legitimate privacy purposes and criminal activities.[4]

Copyright infringement becomes relevant where users exploit these technologies to reproduce or distribute protected works without authorisation. Possible examples include unauthorised distribution of films and television programmes, pirated software, electronic books, music, academic publications, photographs and other digital material. The problem is aggravated where infringing material is repeatedly uploaded by different users or where multiple mirror services emerge following the closure of an earlier website.

An important characteristic of digital piracy is its ability to reproduce itself. Removing one copy does not necessarily eliminate other copies. A copyrighted film removed from one server may already exist on several other servers or be possessed by hundreds of users. Consequently, copyright enforcement increasingly involves not only removing individual files but also addressing the infrastructure through which repeated infringement is facilitated.

5. Copyright Infringement in the Digital Environment

Copyright law generally protects the expression of original literary, dramatic, musical and artistic works, cinematograph films and sound recordings, among other subject matter. Digitalisation does not remove these rights. Instead, it changes the technological means through which infringement occurs.

Section 51 of the Copyright Act, 1957 provides the central statutory framework concerning infringement. Unauthorised reproduction, distribution and other acts falling within the exclusive rights of the copyright owner may constitute infringement. Section 52, however, recognises specified exceptions. These include fair dealing for purposes such as private or personal use including research, criticism or review and reporting current events, subject to the statutory conditions.[5]

This distinction is particularly important in relation to the Dark Web. The anonymity of a user does not automatically convert a lawful use into an unlawful one. For example, a researcher

[4] UNODC, *Darknet Cybercrime Threats to Southeast Asia* (n 1) 8–10. The report notes that darknet technologies have both legitimate privacy uses and criminal applications.
[5] Copyright Act 1957, s 52(1)(a). The statutory exceptions include fair dealing for private or personal use including research, criticism or review and reporting current events, subject to the statutory framework.

using privacy-enhancing technology for legitimate research does not become an infringer merely because the research is conducted through an anonymous network. Copyright liability must still be determined according to the applicable statutory rights and exceptions.

At the same time, the existence of lawful exceptions does not legitimise systematic commercial piracy. A Dark Web service that is established primarily to distribute unauthorised copies of films, books or software may present a very different legal situation from an individual using an anonymity network for legitimate purposes.

The Indian Copyright Act also recognises the increasing importance of technological protection. Section 65A criminalises certain acts of circumvention of effective technological measures where the circumvention is undertaken with the intention of infringing copyright. Section 65B deals with the unauthorised removal or alteration of rights-management information and subsequent distribution or communication of works with knowledge of such alteration.[6]

These provisions demonstrate that Indian copyright law is not technologically neutral in the narrow sense of ignoring digital methods. Nevertheless, technological protection provisions primarily address particular forms of circumvention and rights-management interference; they do not by themselves solve the problems of attribution, jurisdiction and evidence presented by anonymous networks.

6. Why the Dark Web Creates Special Enforcement Challenges Anonymity and Attribution

The first difficulty concerns attribution. Conventional copyright enforcement often begins by identifying a website operator, uploader, hosting provider or user. Dark Web architecture can make such identification substantially more difficult because onion services may conceal server location and users may employ additional privacy-enhancing tools.

Anonymity does not necessarily mean perfect or permanent invisibility. Investigative techniques, operational mistakes, financial records, server seizures, undercover operations,

[6] Copyright Act 1957, 65A–65B. Section 65A addresses circumvention of effective technological measures with an intention to infringe copyright, while s 65B addresses unauthorised alteration or removal of rights-management information.

metadata and other evidence may sometimes allow investigators to identify participants. Nevertheless, the legal significance of anonymity lies in the increased resources and investigative steps required before attribution can be established.

For copyright litigation, this creates a practical problem. A copyright owner may know that a protected work is being distributed without authorisation but may not know who is responsible for uploading or distributing it. The traditional model of suing an identifiable defendant becomes considerably less effective when the operator is unknown.

Jurisdictional Problems

Copyright is principally territorial, whereas the internet is global. A copyrighted work may belong to an Indian copyright holder, be uploaded by an individual located in another country, stored on a server in a third country and accessed by users throughout the world.

This creates several jurisdictional questions. Which country's copyright law applies? Which court has jurisdiction? Where did the infringement occur? Where is the infringing server located? Where did the economic injury occur? Can a domestic injunction be enforced against a foreign operator?

The Delhi High Court recognised this difficulty in *UTV Software Communication Ltd v 1337X.to*, where it observed that international digital piracy becomes considerably more difficult where infringing websites are located outside the jurisdiction and effective enforcement requires cooperation from foreign governments.[7]

International instruments such as the Berne Convention, TRIPS Agreement and WIPO Copyright Treaty establish international standards of copyright protection, but they do not create a single global copyright court or a universal enforcement authority. Consequently, international cooperation remains crucial.

Problems of Digital Evidence

[7] *UTV Software Communication Ltd v 1337X.to* [2019] SCC OnLine Del 8002, CS(COMM) 724/2017, judgment dated 10 April 2019, paras 72, 99–101. The Delhi High Court specifically discussed the difficulty of enforcing copyright against foreign piracy websites and the importance of foreign governmental cooperation.

Copyright enforcement depends upon evidence establishing ownership, copying, distribution, communication to the public and the identity or role of the alleged infringer. Digital evidence may be fragile because websites can disappear, servers can be relocated and content can be modified or deleted.

The evidentiary problem becomes more complicated when the relevant infrastructure is located abroad. Investigators may need cooperation from foreign service providers, domain registrars, hosting companies or law-enforcement agencies. Delays in obtaining such evidence may allow operators to destroy or relocate relevant data.

Accordingly, digital forensic capacity becomes an important part of copyright enforcement. The challenge is not simply finding an infringing file but preserving evidence in a form capable of satisfying the evidentiary requirements of judicial proceedings.

8. Intermediary Liability and Safe Harbour

Intermediary liability represents one of the most difficult areas of digital copyright law. Internet service providers, hosting providers, search engines, platforms and other intermediaries may facilitate communication without themselves creating the allegedly infringing content.

Section 79 of the Information Technology Act, 2000 provides conditional protection to intermediaries from liability for third-party information, data or communication links, subject to statutory requirements.[8]

The Supreme Court's decision in *Shreya Singhal v Union of India* is central to understanding intermediary liability in India. The Court interpreted the expression “actual knowledge” under section 79 in a manner that prevented intermediaries from being required to independently determine the legality of every item of third-party content. The Court held that the relevant obligation arose through a court order or government notification within the constitutional framework considered in that case.[9]

Copyright litigation subsequently developed a more specialised approach. In *MySpace Inc v Super Cassettes Industries Ltd*, the Delhi High Court examined the relationship between

[8] Information Technology Act 2000, s 79. Section 79 provides conditional exemption from liability for intermediaries concerning third-party information, data or communication links, subject to statutory conditions.
[9] *Shreya Singhal v Union of India* (2015) 5 SCC 1, paras 111–119. The Supreme Court considered s 79 and read down the concept of “actual knowledge” in the context of the constitutional challenge before it.

section 79 of the IT Act and section 51 of the Copyright Act. The Court held that sections 79 and 81 of the IT Act and section 51(a)(ii) of the Copyright Act had to be read harmoniously and considered the significance of actual knowledge in the context of specific infringing works.[10]

This approach illustrates an important principle: intermediary liability should not be treated as equivalent to the liability of a primary infringer. A service provider that merely provides technical infrastructure may occupy a different legal position from an operator whose principal purpose is to facilitate copyright infringement.

The distinction becomes particularly significant on the Dark Web. If an anonymous service is intentionally established for distributing pirated works, its legal character may differ from that of a neutral infrastructure provider that unknowingly facilitates a user's communication.

9. Website Blocking and the Indian Judicial Response

Website blocking has become an important component of Indian copyright enforcement. The leading decision is *UTV Software Communication Ltd v 1337X.to*, decided by the Delhi High Court in 2019.

The case concerned websites that allegedly facilitated unauthorised access to cinematographic works. The Court examined the concept of "rogue websites" and considered whether websites predominantly engaged in copyright infringement could be blocked in their entirety. It ultimately granted injunctions against the identified websites and directed relevant authorities and internet service providers to block access.[11]

The significance of the case lies not merely in ordinary website blocking but in the Court's treatment of rapidly multiplying mirror and redirect websites. The Court recognised the problem of "hydra-headed" websites, where a blocked website may reappear under a different domain or through a mirror or redirect address.

---

[10] *MySpace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382, paras 40, 68. The Delhi High Court held that sections 79 and 81 of the IT Act and s 51(a)(ii) of the Copyright Act should be read harmoniously and considered actual knowledge in the context of intermediary liability.

[11] *UTV Software Communication Ltd v 1337X.to* (n 7), paras 1–2, 72, 107. The Court examined "rogue websites", website blocking and the treatment of mirror and redirect websites.

The Court therefore permitted the copyright owners to seek implement of mirror, redirect and alphanumeric websites under Order I Rule 10 of the Code of Civil Procedure, subject to supporting evidence and judicial scrutiny. This mechanism has subsequently been described as a form of dynamic injunction.[12]

The significance of dynamic injunctions is practical. Requiring a copyright owner to initiate an entirely new proceeding every time an infringing website changes its domain could make enforcement excessively slow. At the same time, unrestricted blocking without judicial oversight could create risks of over-blocking. The Delhi High Court therefore stressed that there should be judicial scrutiny and that ISPs should not become arbiters of disputed content.[13]

The UTV judgment consequently illustrates the tension at the heart of online copyright enforcement: effective protection requires speed, but legal legitimacy requires procedural safeguards.

10. Website Blocking and the Dark Web

The effectiveness of conventional website blocking is more uncertain in relation to Dark Web services. Surface-web blocking commonly operates through mechanisms involving domain names, URLs, DNS infrastructure or ISP-level access restrictions. Dark Web services, particularly onion services, operate differently.

Blocking a conventional domain may therefore be technically and legally different from dealing with an anonymous service operating through a privacy-oriented network. Moreover, even where one service is successfully removed, copies of the underlying material may continue to exist elsewhere.

This demonstrates an important limitation of website blocking. Blocking addresses **access to an identified location**, but copyright infringement is ultimately an activity involving copying, distribution and communication of protected works. Consequently, blocking should be treated as one enforcement tool rather than a complete solution.

---

[12] Mohit Panchal, 'Combatting digital piracy in cinematographic works: Delhi High Court grants India's first dynamic injunction against rogue websites' (2019) 14(8) *Journal of Intellectual Property Law & Practice* 596–597.

[13] *UTV Software Communication Ltd v 1337X.to* (n 7), paras 99–101. The Court emphasised that judicial scrutiny was necessary because of the wider implications of site-wide blocking and that ISPs should not become arbiters of infringement disputes.

The Indian experience with rogue websites nevertheless demonstrates that judicially supervised blocking can form part of a broader enforcement strategy. The UTV judgment itself acknowledged both the usefulness and limitations of blocking and stressed the importance of judicial scrutiny.[14]

11. International Copyright Framework

Copyright protection in the digital environment cannot be understood exclusively through national law. The Berne Convention provides the foundational international framework for copyright protection, while the TRIPS Agreement establishes minimum standards of intellectual-property protection and enforcement for WTO members.

The WIPO Copyright Treaty is particularly important because it expressly addresses the digital environment. It recognises the need for copyright protection in circumstances where works are communicated and distributed through digital networks.[15]

However, international copyright treaties do not eliminate jurisdictional boundaries. Enforcement remains substantially dependent upon national institutions, domestic courts, investigative authorities and mechanisms of international cooperation.

The Budapest Convention on Cybercrime is another important international instrument concerning cybercrime investigation and cooperation, although India has not become a party to the Convention. Its significance illustrates a broader point: effective enforcement against technologically sophisticated online activity requires mechanisms for preservation of electronic evidence, mutual assistance and cross-border investigation.

The Dark Web therefore exposes a structural weakness in territorial copyright enforcement. The legal right may be clear, but enforcement can become difficult when the relevant actors, infrastructure and evidence are dispersed across several jurisdictions.

[14] Radha Ranjan et al., 'Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches' in Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches 217–263 (IGI Global Scientific Publishing, 2026), DOI: 10.4018/979-8-3373-5992-2.ch007.

[15] WIPO Copyright Treaty 1996, arts 6 and 8. WIPO explains that the Treaty supplements the Berne Convention and addresses copyright in the digital environment, including distribution and communication to the public.

12. Comparative Perspective: The United States and Notice-and-Takedown

A comparative examination of the United States demonstrates another approach to intermediary liability. Section 512 of the Digital Millennium Copyright Act (DMCA) creates safe harbours for qualifying online service providers, subject to specified conditions. One important mechanism is the notice-and-takedown procedure through which copyright owners may notify service providers of allegedly infringing material.[16]

The American model illustrates the attempt to balance two competing objectives: protecting copyright owners while preventing intermediaries from being automatically liable for everything uploaded by their users. The system also includes a counter-notification procedure in specified circumstances.

However, notice-and-takedown mechanisms have obvious limitations when applied to anonymous Dark Web services. A copyright owner may be unable to identify the responsible service provider or communicate with an operator who deliberately conceals its identity. Similarly, the effectiveness of takedown depends upon the existence of an identifiable intermediary capable of receiving and responding to a notice.

Thus, conventional notice-and-takedown systems are particularly useful where a functioning intermediary exists but are less effective where the infringing infrastructure is deliberately anonymous and resistant to ordinary legal communication.

13. Privacy, Freedom of Expression and the Danger of Over-Enforcement

Any proposal to strengthen copyright enforcement on the Dark Web must recognise that anonymity is not inherently unlawful. Privacy-enhancing technologies may serve legitimate social and democratic purposes.

For example, journalists may need anonymous communication with sources; whistle-blowers may require protection from retaliation; activists may operate in environments where

[16] Gulati, Jivantika, and Radha Ranjan. “Investigating the Relevance and Effects of Performing Rights in Intellectual Property Rights.” 27 Bhairavi Sangeet Sodh Patrika 281–289 (2022). ISSN 0975-5217.

surveillance creates genuine risks; and ordinary individuals may wish to protect personal information from pervasive commercial monitoring.

Therefore, a legal framework that treats anonymity itself as evidence of illegality would create serious concerns. The proper legal target should be **infringing conduct**, not anonymity as such.

A similar concern arises with website blocking. Excessively broad blocking may inadvertently restrict lawful content hosted on the same infrastructure. The UTV judgment recognised the need for judicial scrutiny because site-wide blocking can have wider implications.[17]

Indian constitutional principles also make procedural safeguards important. In *Shreya Singhal*, the Supreme Court emphasised the importance of legal standards and safeguards in the regulation and blocking of online information.[18]

Consequently, copyright enforcement should be designed around proportionality, evidence and judicial supervision rather than indiscriminate technological suppression.

16. Conclusion

The Dark Web presents a distinctive challenge to copyright enforcement not because copyright principles cease to apply in anonymous digital environments, but because the technological conditions under which infringement occurs can make those principles considerably more difficult to enforce. Copyright infringement remains legally relevant irrespective of whether a work is distributed through an ordinary website or an anonymity-oriented network. The central challenge is therefore one of **attribution, evidence, jurisdiction and enforcement**.

Indian copyright law provides a substantial legal foundation. The Copyright Act, 1957 recognises infringement, civil remedies and criminal liability, while sections 65A and 65B respond to certain technological forms of copyright protection. The Information Technology Act provides an intermediary-liability framework, while Indian judicial decisions have progressively developed mechanisms for addressing online piracy.

The decision in *UTV Software Communication Ltd v 1337X.to* is particularly significant because it demonstrates the Indian judiciary's willingness to adapt traditional remedies to the

[17] *UTV Software Communication Ltd v 1337X.to* (n 7), paras 99–104.

[18] Bheem Singh Meena, Radha Ranjan and Shyam Kumar Anand, 'Virtual Meetings under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era' (2023) 4(2) ShodhKosh: Journal of Visual and Performing Arts 1256–1263.

technological reality of online piracy. The development of dynamic injunctions and judicially supervised blocking responds to the problem of mirror and redirect websites. Nevertheless, these remedies cannot completely solve the challenges posed by anonymous and transnational networks.[19]

The future of copyright enforcement on the Dark Web therefore lies in a combination of legal and technological strategies. Stronger digital forensics, faster international cooperation, judicially supervised blocking, carefully designed intermediary obligations and technological protection mechanisms can collectively improve enforcement.

At the same time, the objective should not be to eliminate anonymity or privacy-enhancing technologies. Such technologies can serve legitimate social and democratic purposes. A proportionate legal framework should instead distinguish between the **technology itself and the unlawful conduct committed through it**.

Ultimately, the challenge posed by the Dark Web demonstrates that copyright law must remain technologically adaptive while retaining its fundamental legal safeguards. The objective should be to develop an enforcement system capable of protecting authors, creators and copyright owners without converting the pursuit of digital piracy into unrestricted surveillance or censorship. The most sustainable approach is therefore one that combines legal certainty, technological expertise, international cooperation and judicial oversight.

[19] *UTV Software Communication Ltd v 1337X.to* (n 7), paras 99–107. See also Mohit Panchal (n 12) 596–597.