International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 4 , April 2026
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos

The Convergence of Connectivity and Law: Navigating Intellectual Property Rights in IoT-Enabled Systems

Ram Praveen[1]
[1] *Student, Presidency Uiversity, Bengaluru.*

Article Info

Article History:

Published:30 April 2026

Publication Issue:
Volume 3, Issue 4
April-2026

Page Number:
295-303

Corresponding Author:
Ram Praveen

Abstract:

The Internet of Things (IoT) represents a technological landscape that leads to a paradigm in which billions of connected devices—from commercial sensors and smart appliances to autonomous vehicles and healthcare products—constantly generate, transmit, and generate system data. This convergence of physical and digital environments provides an opportunity to address new and complex issues that have not been largely addressed in relation to the existing Intellectual Property Rights (IPR) framework. This paper explores the structural flaws of contemporary highbrow object doctrines—including patent laws, copyright, confidentiality of transfers, and ownership of facts—as they relate to the layered, distributed, and often computerized nature of IoT systems. The guiding research question for this study is: how should current artificial intelligence paradigms be re-examined to address the specific ownership, authorship and security requirements of IoT environments? Employing a pedagogical approach, the paper analyzes the number one tools of crime, judicial pronouncements, and comparative jurisprudence from India, the United States, and the European Union. It advances three key arguments: first, that multiple IoT system settings generate overlapping and often conflicting IP claims that traditional doctrines cannot address 2nd, that device-generated data and AI-assisted innovations in IoT ecosystems can drive key authorship and manufacturing rules; and 0.33, that the to-jurisdictional nature of the flow of IoT computations requires globally consistent IP governance supported by strong enforcement mechanisms. The paper concludes with a series of doctrinal reforms, including maintaining access to sui generis documents, extended organizational licensing for IoT-generated content, and non-technological compliance characterization, as important responses to the immediate convergence of integration and regulation.

Keywords: Internet of Things (IoT); Intellectual Property Rights; Data Ownership; Patent Law; AI-Generated Innovation

1. Introduction

The Internet of Things (IoT) has emerged as one of the biggest technological trends of the twenty-first century. By incorporating the concept of computation into typical physical objects and connecting them through interactive conversation platforms, IoT systems have dissolved the traditional tensions between tangible and tangible objects. Industrial equipment, household appliances, outdoor equipment, agricultural products, and concrete products now represent a self-sustaining, self-sustaining information age and network environment.

According to statistics, there are more than fifteen billion connected devices in the world, a knowledge that will exceed thirty billion by means of this decade's shutdown.[1]

This increase has major implications for highbrow product development. IP frameworks—traditionally used to oversee discernible human creativity and manufacturing practices—face very different challenges in IoT environments: devices generating patentable improvements, data with fuzzy ownership, software programs embedded in all connected hardware layers, and algorithms learning and adapting in a non-human way standing. The character infrastructure of copyrights, patents, trade secrets and trademark law has changed to one that is open to unique global products and identifiable authors. IoT technology produces fragmented and extracted global processes, and the distance between crime study and technological disruption is growing.[2]

This paper proceeds as follows. Section II maps the technical characteristics of the IoT installation as a basis for subject evaluation. Sections III through VI study specific IP doctrines—patents, copyrights, trade secrets and techniques, and ownership of statistics—in relation to the IoT panorama. Section VII examines comparative judgment results. Section VIII successively modifies the doctrine. Section IX deals with international harmony, and Section X concludes with general reflections on the future of IP law in a highly interconnected world.

2. The IoT Architecture: A Legal Taxonomy

Understanding the IP demand issues posed by the IoT system requires an understanding of its technological mechanisms. IoT systems operate across all 3 interconnected layers: the conceptual layer (physical sensors and applications), the web layer (communication protocols and records transmission infrastructure), and the value layer (cloud platforms, analytics engines, and user interfaces). Each layer harbors remarkable intellectual curiosity and generates a strange variety of legitimately recognized outcomes.[3]

In the intellectual space, IP optics compete with hardware design, embedded firmware, sensor technology, and proprietary calibration algorithms. In the local environment, values encompass conversational methods, encryption techniques, and data analysis techniques. At the application layer, more complex legal terrain emerges: real-time data generation, device pattern recognition learned from application data, user data generation, and the emergence of automated selection processes all converge for crime detection in current IP classes.[4]

Thus, the taxonomy of IoT-related intellectual property includes: (i) novel hardware that can be protected by patent and design law; (ii) embedded software that can be protected with the help of copyright; (iii) proprietary data, unquestionably, under trade secret laws or sui generis emerging data regimes; (iv) AI outputs whose

[1] *Ericsson Mobility Report (November 2023) (Ericsson 2023), projecting IoT connected device growth globally.*
[2] *Ryan Calo, "Privacy in the Age of Robotics" (2011) 17 Journal of Internet Law 3, examining distributed technology and law.*
[3] *Luigi Atzori, Antonio Iera, and Giacomo Morabito, "The Internet of Things: A Survey" (2010) 54(15) Computer Networks 2787*
[4] *World Intellectual Property Organization, Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence (WIPO 2020).*

authorship and ownership remain doctrinally disputed; and (v) labels and certification marks used in related product life cycles. This structural flexibility is not only of technical importance; it is far from the most intractable IP conflicts within the IoT space.[5]

3. Patent Law and IoT Innovation: Fragmentation and Conflict

Patent law has evolved into one designed to motivate human inventors by granting excessive levels of protection to new, obscure, and industry-related innovations. In the IoT framework, this framework faces at least three structural challenges: the challenge of overlapping patents, the patentability function of software and standards, and the emerging question of AI-assisted or AI-produced products.[6] An Single IoT device can have a wide range of patentable technologies—chipset architectures, wireless conversation requirements, sensor calibration methods, facts encryption algorithms, and user interface mechanisms. This phenomenon of patch accumulation or patch sprouting poses significant challenges to market access and coordination. Standard-important patents (SEPs), which cover new technologies included in speech exchange requirements including Bluetooth, Zigbee and 5G NR, are particularly difficult. SEP holders are required under FRAND (Fair, Reasonable, and Non-Discriminatory) licensing covenants, yet litigation over FRAND royalty fees has proliferated around the world, with courts in the United States, Germany, China and India taking different approaches.[7] The patentability of software software innovations—a key enabler of the IoT—remains an inconsistent legal process. In the United States, the Supreme Court's choice in Alice Corp. v. CLS Bank International (2014) established a -step test that resulted in patent invalidation of many software, creating uncertainty for IoT builders whose innovations are exclusively software-based.[8] Perhaps maximum based, output AI-assisted invention demanding situations the human inventorship requirement. If an IoT device automatically generates a single structure that satisfies the criteria for patentability, the question of who — or what — is the designer remains legally unresolved. The UK Supreme Court's choice in Thaler v. Controller-General of Patents (2023) held that an AI machine cannot be named as an inventor under the Patents Act 1977, leaving a doctrine in which indeed device-driven IoT advances can additionally get out of the gate patent protection altogether.[9]

[5] European Union Intellectual Property Office (EUIPO), Trends and Developments in Artificial Intelligence (2021).

[6] *Patents Act 1970 (India) ss 2(1)(j), 3(k); 35 USC § 101 (US)*; European Patent Convention art 52.

[7] *Unwired Planet International Ltd v Huawei Technologies Co Ltd [2020] UKSC 37; Ericsson v Intex Technologies (India) CS(OS) 1045/2014 (Delhi HC).*

[8] *Alice Corp v CLS Bank International 573 US 208 (2014).*

[9] *Thaler v Comptroller-General of Patents, Designs and Trade Marks [2023] UKSC 49.*

4. Copyright and IoT: The Authorship Deficit

Copyright law's fundamental requirement for a human author poses significant challenges for IoT environments, where the growing amount of secure data including firmware updates, data visualizations, analytics reports, and even printouts by AI-powered IoT gadgets — are available with minimal human innovation guidance. This preliminary requirement, set out under the Indian rules in Eastern Book Company v DB Modak (2008) and the US in Feist Publications v Rural Telephone Service Co (1991), needs more than machine gathering or algorithmic aggregation.[10] The embedded software software — the life of the IoT devices — can be protected by copyright just like text images under both the Indian Copyright Act, 1957 and the Berne Convention. However, the implementation of software software copyright enforcement in IoT ecosystems is difficult through the layering of application architecture. Combined open source software, middleware, and custom exploitation code often coexist in a single container, creating complex licensing stacks in which GPL, MIT, Apache, and licensing work must be completed simultaneously. Failure to comply with open source licensing—a recognized trend within the IoT hardware space—can expose manufacturers to copyright law responsibilities that do not fit the nature of the infringement.[11] Documents generated by IoT devices present another challenge to copyright. Raw sensor data—temperature readings, regional coordinates, biometric measurements—lack the priority necessary for copyright protection. However, generated data, learned machine management models, and output estimates from such data can also be protective, relying on the degree of human innovation selection and planning involved. The EU Communications Directive (ninety-six/nine/EC), which provides sui generis protection for communications representing a full investment, provides a partial example, although its application to dynamic, real-time IoT communications remains relatively static.[12]

5. Trade Secret Law and IoT Data Flows

In the absence of strong patent and copyright protection for IoT-enabled codes and algorithms, the development of exchange secrets has emerged as a critical protection strategy for IoT innovators. The financial value of IoT facts no longer lies in their qualities—which can often be insecure—but in the patterns, correlations, and predictive predictions that can emerge from years of accumulation and analysis. These intellectual findings are

[10] *Eastern Book Company v DB Modak (2008) 1 SCC 1; Feist Publications Inc v Rural Telephone Service Co 499 US 340 (1991).*
[11] *Copyright Act 1957 (India) ss 2(o), 14(b); Berne Convention for the Protection of Literary and Artistic Works (adopted 9 September 1886, revised Paris 1971) art 2*
[12] *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases [1996] OJ L 77/20.*

routinely described as mysterious changes and mechanisms in national legislations implementing the minimum requirements of the TRIPS Agreement on the protection of undisclosed data.[13]

India's exchange confidentiality protection is often based on unusual legal concepts of breach of self-reliance supplemented by the relief of contractual protection. The Digital Personal Data Protection Act, 2023, initiates important tasks regarding the use of personal facts generated by IoT devices, but no longer immediately addresses the economic measurement of IoT records as an additional confidential asset. In contrast, the USA Defend Trade Secrets Act (DTSA), 2016 provides a federal civil cause of action for trade secret infringement and has been applied to IoT-related disputes involving attacks on sensor data and device reading models.[14]

The fundamental challenge in protecting the confidentiality of IoT exchanges lies between the legitimate interest of IoT users in protecting the confidentiality of potentially competitive data, and the emerging regulatory importance of document portability and interoperability. The EU Communications Directive (Regulation 2023/2854), which entered into force in 2024, gives IoT users the right to access and share statistics from devices, enabling changes to privacy protection that are important for the goals of resistance and open innovation. This direct alignment between IP security and copyright law represents a very broad legal frontier within the IoT space.[15]

6. The Data Ownership Problem

Perhaps the most fundamental issue with the IoT-assisted IP project deployed is the lack of a clear framework on ownership of documents. Unlike physical objects or traditional IP assets, facts are not currently ideally structured in object standard groups: less conflicting (can be used simultaneously through multiple cases), permanent (functionality no longer breaks it), and no problem to replicate at minimal cost. Current criminal frameworks cannot accurately answer the seemingly fundamental question of who owns the data generated by an IoT application: the developer, the platform operator, the terminator, or the subject of the documents.[16]

This ambiguity of ownership has significant commercial and criminal implications. Manufacturers claim ownership, through separate contractual exclusion clauses in license agreements (EULAs). Platform operators assert manage via their role as facts processors and aggregators. Users acquire behavioral information through their interactions with devices and argue for information autonomy. Where documentation code can be identified—because often in patron IoT—accounting protection law, the EU GDPR and the India Digital Personal

[13] *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (Marrakesh, 15 April 1994) art 39.*

[14] *Defend Trade Secrets Act 2016 (US) 18 USC § 1836; Digital Personal Data Protection Act 2023 (India).*

[15] *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act) [2023] OJ L 2023/2854*

[16] *Lothar Determann, "No One Owns Data" (2018) 70 Hastings Law Journal 1; Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1 art 4.*

Data Protection Act, 2023, provides conflicting facts about rights of access, rectification, and deletion that coexist seamlessly with manufacturer industry data requirements.[17]

Resolving the question of access to information calls for a sui generis felony framework that acknowledges the penetration of IoT data by multiple parties. A layered ownership version — in which real data rights challenge users to non-exclusive licenses granted to manufacturers and platform operators for specific purposes — would more accurately reflect the distributed reality of IoT computing time than current contractual terms. The EU Data Protection Regulation, which includes access rights to documents, although not current property rights, represents a step in this direction beyond legally enforceable rights to fact-sharing that operate independently of contracts.[18]

7. Comparative Jurisdictional Responses

The panoramic legislation governing IoT and highbrow products is divided into jurisdictions, reflecting differing coverage priorities and felony customs. A comparative study of India, the United States and the European Union is famous for the extent of this merger and the possibilities for alignment[19]. In India, there are no precise IoT intellectual property laws, meaning the art is governed by something called the Patents Act, 1970, Copyright Act, 1957, Information Technology Act, 2000, and Digital Personal Data Protection Act, 2023. The Department of Industry and Internal Trade Promotion (DPIIT) has acknowledges IP problems but dispenses with temporary legal remedies. Litigation innovation has been hampered by a decline in IoT-unique IP litigation, though the Delhi High Court's rulings on software patentability and the Supreme Court's broad clarity on change privacy protection under the self-service law provide a growing foundation[20]. The United States adopted a largely market-led approach. The Federal Trade Commission exercised oversight authority over the use of IoT labels in its consumer protection order. The National Institute of Standards and Technology (NIST) has released cybersecurity standards for IoT devices. Patent litigation involving IoT technologies has become a major issue, with the Patent Trial and Appeal Board becoming an important forum to challenge the infringement of IoT-associated patents thru inter partes evaluate proceedings. The absence of a comprehensive federal IoT or ownership of facts law creates significant uncertainty for criminals, especially for small and medium-sized IoT businesses[21].

[17] *Digital Personal Data Protection Act 2023 (India) ss 6–12*; GDPR (n 16) arts 15–20.

[18] *Data Act (n 15) arts 4–6*; European Commission,

[19] *OECD, "Going Digital: Shaping Policies, Improving Lives" (OECD Publishing 2019).*

[20] Department for Promotion of Industry and Internal Trade (DPIIT), Draft National Policy on Internet of Things (Government of India 2023).

[21] Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World (FTC 2015).

8. Proposed Doctrinal Reforms

The analysis in the previous chapters is the 4 most important named regions where academic reform is essential to take highbrow belongings regulation in line with IoT reality in the best possible way. First, a sui generis document access framework should be established at national level, modeled in part on the EU data regulation but adapted in real time for mechanical IoT data. This framework should grant rights to original documents within the consumer on a market-free license basis for manufacturers and platform operators, with specific barriers to secondary industrial use and clean standards for the use of considerations. The Law Society of India and the Ministry of Internet and Communications are well placed to develop any such framework as a complement to the Digital Personal Data Protection Act, 2023.[22]

Second, the 1970 patent law should be amended to create an impartial invention rule in which AI-assisted and AI improvements are granted to the human operator or installer of the AI device, rather than the need to recognize a self-selected inventor. This approach, consistent with WIPO's discussion ideas on artificial intelligence and artificial intelligence, could circumvent the learning curve that currently leaves AI's IoT success untouched by any prisoner.[23]

Third, an extended organizational accreditation mechanism should be established to use IoT-generated literature for learning models. Based on the Nordic prolonged collective licensing version and the EU Digital Single Market Directive rules for records and facts, this kind of technology could allow AI builders access rights to IoT-generated datasets under popular terms communicating with representative amassing societies attribution mechanisms) clearly.[24]

9. International Harmonisation

The trans-jurisdictional nature of IoT emergence makes global coordination no longer just relevant, but essential. IoT devices are designed in one region, manufactured in another, processed in a 3rd layer, and produced documents processed in a fourth layer. The law applicable to any given IP dispute may come from the design,

[22] *Law Commission of India, "Report on Legal Framework: Ease of Doing Business" (Report No 275, 2022)*; Digital Personal Data Protection Act 2023 (India).

[23] WIPO, Conversation on Intellectual Property (IP) and Artificial Intelligence (AI): Third Session (November 2020) WIPO/IP/AI/3/GE/20.

[24] Directive (EU) 2019/790 on Copyright in the Digital Single Market [2019] OJ L 130/92 arts 3–4.

architecture, service, or document usage domain, and the cut-throat guidelines of specific international laws provide endless driving guidance for these many surrounding nodes.[25]

The World Intellectual Property Association provides the most appropriate local discussion forum to develop a global instrument on IoT intellectual property. Based on the WIPO Copyright Convention (1996) and the WIPO Convention on Use and Phonograms (1996), the new WIPO IoT Convention may impose minimum requirements: (i) patentability of IoT innovations, including software innovations (ii) copyright protection in embedded IoT data and software; (iii) sui generis facts discovery rights; and (iv) transit boundary enforcement mechanisms. India, as a major IoT manufacturer and consumer and a member of both WIPO and WTO, is well placed to address this type of initiative in the Global South.[26]

Bilateral and regional trade agreements provide the perfect avenue for further harmonization. The India-EU Free Trade Agreement, which is currently under negotiation, and India's association with the ASEAN Digital Economy Agreement each offer opportunities to incorporate IoT IP standards into broader economic sectors. Such multidimensional approaches have historically been effective in advancing IP research, as tested by the emergence of the TRIPS Agreement in Uruguay's integration negotiations.[27]

10. Conclusion

The Internet of Things has arrived for a second, when intellectual property law isn't quite ready to receive it. A framework designed to protect new identifiable acts of human authors and producers is now required to examine the results of endowed, independent, and empirical knowledge on technological systems, whose complexity militates against the relative classifications to which IP doctrine applies. The character gaps identified in this paper—copyright deficit, patent reform deficit, ownership gap in facts law, and split enforcement in cross-border IP disputes—are not isolated questions but social problems with real outcomes for innovators, customers, and public policy.

The recommendations outlined in this paper—a sui generis information system, AI-adaptive inventorship provisions, extended organizational licenses for IoT assessments, and worldwide harmonization of compliance measures—represent an important first step towards a transparent prison architecture in the IoT era. They are not generally a rethinking of IP law but rather a deliberate reassessment of current doctrines to account for the precise characteristics of interconnected, automated, and informed systems. Required counseling is not just criminal, but financial and regulatory: in the real economy, a growing number of people with the help of IoT-generated records

[25] *Peter Drahos, A Philosophy of Intellectual Property (Dartmouth 1996)*; Paul Torremans (ed), Intellectual Property and Private International Law (Edward Elgar 2008).

[26] *TRIPS Agreement (n 13); ASEAN, ASEAN Digital Masterplan 2025 (ASEAN Secretariat 2021).*

[27] *Shamnad Basheer, "India's Tryst with TRIPS: The Patent Amendment Act 2005" (2005) 1 Indian Journal of Law and Technology 15.*

and AI-mediated innovation, IP regulation can defend real human creativity and imaginative efforts — even as it may facilitate unfastened glide of facts for technological development—this enables determining the conditions of participation in the information economy for people, enterprises and nations alike.

The collision of relations with law is not always a future to be expected but a present to be addressed. The legislative, judicial and global response to this hearing will require the distribution of the enormous economic and social benefits generated with the help of the IoT environment for decades to return. The time has come for multiplication; The complexity and scale of the IoT industry demands innovation commensurate with the transformation it represents.