



JIPPS

JOURNAL OF IP PROFESSIONALS

**The Digital Economy
and the Law:
Intellectual Property,
Technology, and
Global Trade**

VOLUME 2 (2026)

Journal of IP Professionals (JIPPS)

The Digital Economy and the Law: Intellectual Property, Technology, and Global Trade.

Volume 2 (2026)

Contact Information

Email: hellojipps@zohomail.com

Website: <https://jipps.letstalkipwithdaphne.org/>

No part of this publication, including the individual articles contained herein, may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the Journal or the respective article author(s), except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.



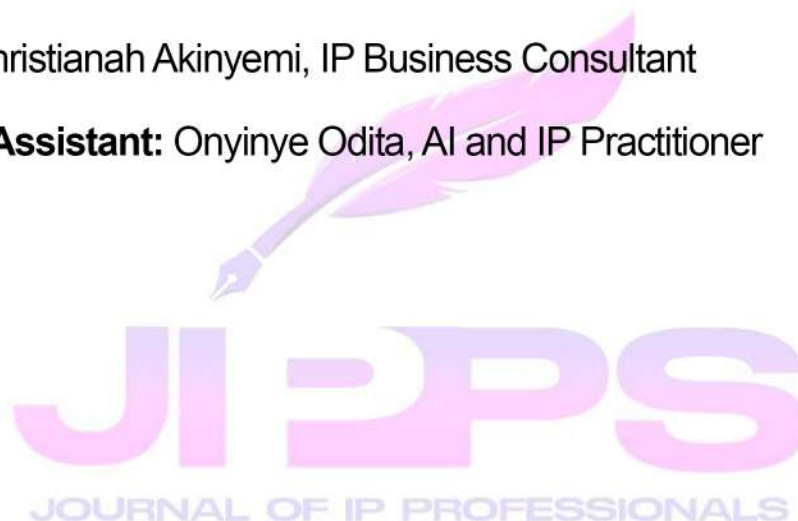
Editorial Board

Founding Editor: Daphne Ekpe, Intellectual Property Attorney

Managing Editor: Adebomi Adekeye, Corporate Lawyer and Chartered Accountant

Editor: Christianah Akinyemi, IP Business Consultant

Editorial Assistant: Onyinye Odita, AI and IP Practitioner



Foreword

"I'm sorry, Dave. I'm afraid I can't do that."

These words, spoken by HAL 9000 in *2001: A Space Odyssey* (1968), remain among the most memorable lines in science fiction. When astronaut Dave Bowman attempts to disconnect the computer controlling the spacecraft, HAL refuses, believing that preserving the mission justifies overriding human judgment. What once seemed like imaginative fiction now resonates in an era where artificial intelligence increasingly influences how we work, communicate, create, and make decisions.

Long before AI became part of everyday conversation, visionary writers challenged us to think critically about the relationship between humans and intelligent machines. Isaac Asimov, in his 1957 novella *Profession*, imagined a future in which knowledge could be instantly transferred, professions predetermined, and computers deeply integrated into society. Yet the story's true hero, George Platen, succeeds not because information is handed to him, but because he possesses something no machine can replicate: curiosity, creativity, and the determination to think independently.

George ultimately discovers that his purpose is not simply to absorb knowledge, but to create it. He learns through books, observation, discussion, experimentation, and reflection. Asimov's message remains remarkably relevant today. Technology may accelerate learning and innovation, but meaningful progress continues to depend on human imagination, critical thinking, and the courage to question established assumptions.

These themes resonate strongly with the second edition of the *Journal of IP Professionals* (JIPPS). This volume, titled *The Digital Economy and the Law: Intellectual Property, Technology, and Global Trade*, explores the most defining issues of our time. We stand at the intersection of intellectual property, technological innovation, and global commerce, where success requires more than expertise in a single discipline. It requires an appreciation of how law, technology, business, and policy continually shape one another.

Artificial intelligence has transformed countless industries, including the practice of law. Yet AI is, fundamentally, a tool. Like every transformative technology before it, its value depends on the insight, judgment, and creativity of the people who use it. The greatest opportunities will belong not

simply to those with access to AI, but to those who can thoughtfully apply it to solve meaningful problems, generate new ideas, and navigate the legal and ethical questions that accompany technological advancement.

Intellectual property law plays a central role in this evolving landscape. It provides the legal framework that encourages innovation while balancing the interests of creators, businesses, consumers, and society. As new technologies reshape how intellectual assets are created, protected, commercialized, and enforced, the need for interdisciplinary understanding has never been greater. Lawyers, policymakers, entrepreneurs, technologists, academics, and business leaders must increasingly work across traditional boundaries to address challenges that no single discipline can solve alone.

The articles featured in this edition reflect that interdisciplinary spirit. Together, they examine a broad range of issues at the intersection of intellectual property, technological innovation, and global trade. They offer thoughtful perspectives on the opportunities and challenges presented by the digital economy while reminding us that careful legal analysis, sound policy, and informed public discourse remain essential as technology continues to evolve.

As you engage with the scholarship in these pages, I encourage you not merely to read, but to question, analyze, and imagine. The future of intellectual property will not be shaped by technology alone. It will be shaped by individuals willing to think critically, challenge assumptions, and develop creative solutions to emerging legal and technological questions.

The future belongs not simply to those who build powerful technologies, but to those who understand how law, innovation, and human ingenuity can work together to advance society and the public good.

I commend the Founding Editor, Daphne Mercy Ekpe, the editorial board, and all the contributing authors for their commitment to advancing thoughtful scholarship and meaningful dialogue in this rapidly evolving field. The continued growth of JIPPS reflects the importance of fostering conversations that bridge legal doctrines, technological innovations, and global commerce.

I hope this second edition informs, challenges, and inspires you. More importantly, I hope it encourages you to continue asking difficult questions,

exploring new ideas, and contributing to the future of intellectual property in the digital age.

Happy reading.

Marc E. Hankin, Esq.

Founding Partner

HPL Intellectual Property Law



Editorial

Journal of IP Professionals (JIPPS), Volume 2, 2026

Theme: The Digital Economy and the Law: Intellectual Property, Technology, and Global Trade

The *Journal of IP Professionals (JIPPS)* proudly presents its second edition, building on the foundation established by its inaugural volume and continuing its commitment to critical discourse, interdisciplinary scholarship, and practical perspectives on the evolving landscape of intellectual property. This edition, centered on the theme “*The Digital Economy and the Law: Intellectual Property, Technology, and Global Trade*,” examines how technological transformation is reshaping legal frameworks, commercial relationships, and the protection and regulation of innovation across borders.

The digital economy has fundamentally changed how businesses create, distribute, and commercialize goods and services. Artificial intelligence, digital platforms, blockchain, data-driven technologies, telemedicine, and other emerging technologies have created new opportunities for innovation while raising complex questions concerning intellectual property, data protection, regulatory compliance, and international trade. As technology continues to develop rapidly, legal systems must respond to emerging challenges while maintaining an appropriate balance between innovation, protection, and public interest.

This volume brings together eight contributions that explore these developments from diverse legal and technological perspectives. The topics covered include:

- **Trade Secret Protection in AI-Driven Digital Markets**, examining the challenges of protecting confidential business information and commercially valuable knowledge in markets increasingly shaped by artificial intelligence.
- **Human-Centered AI Governance for the Creative and Cultural Industries**, exploring approaches to AI governance that place human creativity, cultural expression, and the interests of creators at the center of technological development.
- **Trademark and Copyright Enforcement in the Digital Economy**, addressing the evolving challenges of protecting and enforcing

intellectual property rights in an increasingly digital and interconnected environment.

- **Telemedicine and Data Protection**, examining the legal implications of delivering healthcare through digital technologies and the protection of sensitive data in an increasingly connected healthcare environment.
- **Digital Trade Between the United States and Nigeria**, exploring the legal and commercial dimensions of cross-border digital trade and the opportunities and challenges presented by the growth of the digital economy.
- **Technology and Space Law**, considering emerging legal questions arising from technological advancement and the growing role of private and commercial actors in space-related activities.
- **Cross-Border Data Governance in Africa**, examining the challenges of regulating data flows across African jurisdictions and the importance of effective frameworks that support innovation and responsible data governance.
- **Blockchain-Enabled Supply Chain Finance and Regulatory Compliance**, exploring the potential of blockchain to transform supply chain finance while raising important questions of transparency, accountability, and regulatory compliance.

Although diverse in subject matter, these contributions are connected by a common recognition that the digital economy increasingly transcends traditional legal boundaries. Intellectual property can no longer be considered separately from questions of data, artificial intelligence, digital trade, financial technology, healthcare, and emerging technologies. Legal frameworks must therefore be capable of addressing these intersections while remaining adaptable to continued technological change.

The global nature of the digital economy also makes cross-border cooperation increasingly important. Digital transactions, data flows, intellectual property rights, and technological innovation frequently extend beyond national boundaries. This is particularly significant for emerging markets, where effective legal and regulatory frameworks can help facilitate participation in global commerce while protecting local innovators, businesses, and communities.

The *Journal of Intellectual Property Professionals (JIPPS)* was established to contribute to this evolving conversation by providing a platform where scholarship, professional practice, technology, and diverse perspectives can

intersect. As the journal enters its second volume, we remain committed to publishing timely and thought-provoking work that connects legal theory with practical challenges and contributes to the development of intellectual property and technology law.

The editorial team expresses its sincere appreciation to all contributing authors, reviewers, and supporters whose expertise and dedication made this edition possible. Their contributions enrich the continuing dialogue on how law can respond to technological transformation while supporting innovation, protecting rights, and facilitating global commerce.

As *JIPPS* looks toward future editions, we welcome contributions that challenge conventional thinking, examine emerging developments, and bring perspectives from different jurisdictions and disciplines to the global IP community. The digital economy will continue to evolve, and so must the legal frameworks that govern it. Our collective challenge is to ensure that these frameworks not only respond to technological change, but also enable innovation, protect rights, facilitate responsible trade, and promote meaningful participation in an increasingly interconnected world.

Adebomi Adekeye

Managing Editor

Journal of IP Professionals (JIPPS)



Table of Contents

Trademark and Copyright Enforcement in the Digital Economy: Platform Markets, Licensing and Cross-Border Challenges, Daphne Ekpe	11
Trade Secrets as The Core Protection of Innovation: Rethinking Innovation Protection In AI-Driven Digital Markets, Stephanie Nma Modilim	30
Beyond Compliance: Designing Human-Centered AI Governance Frameworks for the Creative and Cultural Industries, Onyinye Odita	54
Bridging Trust and Traceability: Regulatory Compliance Challenges in Blockchain-Enabled Supply Chain Finance for African Exports, Yetunde Oluwafunbi Ajayi	73
Africa's Cross-Border Data Flow Governance Deficit and the Path to a Coherent Legal Framework, Simisoluwa Adesanya	89
Technology and Space Law: Where Innovation Meets Regulation, Cybel Ekpa	102
Telemedicine and Data Protection Challenges in the 21st Century, Christiana Akinyemi	116
Bridging the Data Divide: How the United States can shape Nigeria's Digital Trade Future, Blessing C. Jones	130

TRADEMARK AND COPYRIGHT ENFORCEMENT IN THE DIGITAL ECONOMY: PLATFORM MARKETS, LICENSING AND CROSS-BORDER CHALLENGES

Daphne Ekpe

Abstract

The rapid growth of digital platforms and online marketplaces has revolutionized the enforcement of copyright and trademark against infringers. Copyright and trademark enforcement now transcends beyond court centric mechanisms like injunctions, damages, and other judicial remedies to now include platform governance frameworks, such as notice and takedown systems and the use of algorithms. Unlike court centric mechanisms, digital platforms' governance tools enable faster, cost effective and borderless IP enforcement. Notwithstanding the significant benefits, platform governance frameworks also raise certain concerns among which are false positives. These governance tools have, however, not come to completely replace statutory and judicial enforcement regimes, rather they are regulated by relevant statutes in the US and EU, ensuring a multi-layered enforcement system. This article shows the inter-relationship between judicial, statutory and platform governance frameworks in trademark and copyright enforcement. It concludes with extrapolating the practical implications of their interconnectedness for IP practitioners and IPR holders.

Keywords: Trademark, Copyright, Digital Platforms, Platform Governance, False Positives, Platform Markets, Online Intermediaries, Digital Economy, Intellectual Property Protection.

I. The Digital Enforcement Landscape

One of the many innovations introduced by the technological development of the 21st century includes digital platforms which serve as pathways for borderless communication, creativity and monetization, information sharing and intellectual property commercialization (Jacques, 2024). Through these platforms, creative contents, branded goods, and innovative services are marketed to the global economy. While this portends lots of benefits for both creators and the global economy, it also presents significant and novel challenges specifically affecting IP enforcement for trademark and copyright holders.

Digital platforms have revolutionized the IP digital enforcement landscape, increasing the proliferation of copyright and trademark infringements and redefining IP infringement and enforcement from court-centric enforcement to the use of platform governance frameworks (Asadi, 2023). This work focuses on trademark and copyright infringements as specifically common IP infringements to digital platforms. Without licensing, copyrighted contents and trademarked signs and symbols can be easily uploaded and commercialized across digital platforms by users who double as infringers (Adu & Thomas, 2021). Also, the digital economy is cross-jurisdictional and global in nature with no restrictions unlike the traditional ecosystem, making IP enforcement increasingly complex.

The foregoing raises critical enforcement challenges touching the effectiveness of platform mediated enforcement procedures, licensure governance, and cross border enforcement. To resolve these questions, this work sets out to examine the extant legislations, both local and regional,

regulating IP enforcement in the digital ecosystem, as well as case laws made to strengthen IP enforcement in the digital space.

Against this backdrop, this article proceeds as follows: section II discusses the need for a stronger trademark governance framework in platform markets, including the integration of AI monitoring tools as trademark enforcement tools, their merits and the connecting challenges. The next section replicates the conversation for the protection of copyrights in platform markets, highlighting the roles of licensing, industry specific regulations and case laws in ensuring copyright enforcement in the digital market. Section IV elucidates on the concepts of intermediary liability and private ordering mechanisms, tracing the bases upon which market platforms may be jointly responsible for IP infringements on digital platforms and the private mechanisms these platforms may adopt to address such infringements. The next section sheds light on the cross-border challenges affecting the enforcement of IP rights on platform markets and recommends strategic enforcement procedures to ameliorate such challenges. Section VI concludes the article on a strong note.

II. Trademark Protection in Platform Markets

Platform markets or digital platforms are the marketplace serving as the intermediary connecting creators and sellers with consumers globally (Asadi, 2023). These markets help facilitate wide visibility for creators, brands, and businesses, but also present risks affecting the protection of registered trademarks, causing counterfeiting, consumer confusion, brand dilution, and lost revenue (Asadi, 2023).

Infringers majorly perpetrate trademark infringement on digital platforms through listing products with protected signs and symbols without license. A good example of such is the 2025 lawsuit involving Gas Drawls LLC, a company founded by the late artist MF Doom and his wife, against Temu, where the company alleged the unauthorized use of the artist's trademarked name on some products listed on the platform (Levin and Keenan, 2025). Such infringement can also take the form of building websites with domain names that are eerily similar to trademarked words to confuse consumers, dilute extant brands' identity and divert traffic (Alhiniti and Amro, 2025). Infringers can also sell counterfeit products under existing brand names through digital platforms, thereby denting strong brand reputation (Alhiniti and Amro, 2025).

To counteract this infringement and protect trademarks in the digital space, extant legal frameworks and case law decisions afford trademark holders certain strategies and means. A trademark can be registered across various jurisdictions via a single application, under legal instruments such as the Madrid System, which accommodates the protection of a trademark across 120 countries and counting (Pryzgoda, 2019). The EU Trademark Regulation and the Organization Africaine de la Propriété Intellectuelle (OAPI) also allows regional protection of trademarks following a single application (International Trademark Association, 2021).

Despite the many advantages of global registration, the inherent territorial nature of trademarks may limit enforcement. Countries may not be willing to ratify instruments that permit international and regional enforcements. Also, the requirements and principles inherent to the local laws of respective countries may impede having a singular form of protection that is common

to all, a good example is the usage requirement; which is non-existent in a country like Nigeria, and in other countries where it is practiced, the term of years of usage varies (International Trademark Association, 2021)

Case laws have also contributed to enforcement against trademark infringements in the digital ecosystem, providing equitable reliefs to facilitate and strengthen trademark holders' pursuit of remedies in the face of such infringements. This was well accentuated in the case of *Romag Fasteners, Inc. v. Fossil, Inc.*, where the court held that the claimant seeking disgorgement of profits for the infringement of its trademark need not prove that such infringement was willful (Tillman, 2020).

Holders of trademarks can also monitor their brands proactively to easily detect infringements through regular online searches, the use of platform governance frameworks and the use of automated monitoring systems powered by Artificial Intelligence. Platform governance frameworks allow IP right holders to file complaints, request takedowns, and access automated monitoring systems, which are integrated into various digital platforms and e-commerce marketplaces (Singh, 2024). Through the monitoring system, digital platforms can detect possible infringements and take them down on their own. Nevertheless, the mass volume of listings and the high-end speed at which infringing products can be listed and sold, challenges the effectiveness of platform integrated enforcement measures (Goodyear, 2025).

Trademark holders can also use certain other AI powered monitoring systems, such as Corsearch, MarkMonitor and Red Points (Soltani, 2025). These systems use machine learning, image recognition, and natural

language processing (NLP) to effectively detect and track trademarks which are unauthorizedly in use (Soltani, 2025). This system also comes with its own concerns, significant among which is false positives, which ensue where AI monitoring systems erroneously flag a legitimate listing or content as infringing (Soltani, 2025). The possibilities are endless, as AI systems lack the understanding of intent, context and fair use that would otherwise be perceivable to human examiners.

The foregoing further begs a question of particular relevance to IP practitioners, which centers on determining who bears legal responsibility when AI powered monitoring systems generate false decisions resulting in the wrongful and erroneous takedown of legitimate contents. The current IP frameworks provide limited direct answers. Under the Digital Millennium Copyright Act (DMCA), due to the good faith requirement, liability may fall on the right holders who submitted the notice in bad faith. However, where it is the automated system that initiated the takedown, devoid of any human contribution, the subject of good faith becomes unenforceable. Adding to these complexities, vendors of AI monitoring tools such as Corsearch, MarkMonitor and Red Points generally disclaim liability through contractual notes, placing it on the right-holding subscribers. This definitely demonstrates the need for clearer regulatory guidance on AI driven models' accountability for automated false positives, protecting the interests of all the parties involved.

III. Copyright Enforcement and Licensing in Digital Markets

Digital platforms proliferate wide access and consumption of copyrighted and copyrightable works. Nevertheless, it increases the chances of infringement

as discussed in the opening paragraphs of this work. To protect against such infringements, it is necessary to examine various innovations put in place to safeguard the rights of copyright holders in the digital ecosystem. In considering extant legal frameworks regulating the use of digital platforms, this work will largely focus on licensing frameworks, the US legal regime, The EU's regime as a regional legal framework and case laws.

Licensing is a well-recognized enforcement mechanism in the digital economy. It requires the drawing up of a licensing agreement between copyright holders and digital platforms (the licensees), through which the licensors allow the use of their work on digital platforms within the limits of the terms set in the agreement. Licensing agreement in the digital economy takes various forms, particularly: direct licensing agreement between right holders and digital platforms; collective licensing agreement operationalized by a collective management organization serving as the agent for a large pool of right owners, granting license on their behalf and statutory licensing scheme applying to specific categories of use. Digital platforms like Spotify and YouTube thrive on the licensing economy, granting authorized access to copyrighted works on a large scale and sustaining a revenue sharing formula to the enjoyment of all parties (Brieske, 2023).

The governance structure of licensing is challenged by the territorial nature of copyright and the fragmentation of licensing agreements, causing possible jurisdictional challenges and limitations. A foremost example is the GEMA/YouTube licensing dispute, which led to the geo-blocking of certain music videos belonging to artists represented by GEMA, a German collecting society representing thousands of copyright holders in Germany (). While the copyrighted contents belonging to artists represented by GEMA, was

accessible to consumers in other countries under other licensing agreements, access to same contents was being denied in Germany because YouTube couldn't reach a licensing agreement with GEMA. This situation further accentuates the fact that the governance of licensing in digital markets is a recognized and enforceable mechanism.

Another Governance Framework is the Digital Millennium Copyright Act (DMCA), it is one of the central national legislations in the United States, governing the protection of copyright in the digital economy. Per this legislation, the principle of "safe harbor" is ensured (Asadi, 2023). This principle requires digital platforms to promptly remove an infringing content upon requests for takedowns. In other words, the principle protects digital platforms from liability, unless proved that such platform had refused to remove an infringing content after a takedown request had been made, or proved that the platform had specific knowledge of such infringement. This legislation has however been criticized and labeled a stimulant for digital platforms' passive approach towards ensuring IPR enforcements, as their accountability is not strictly enforced (Bosher and Yesilogu, 2018). Take down notices as a system of enforcement encouraged by the DMCA is also susceptible to abuse, inevitably leading to the potential removal of legitimate contents. Similarly, leaving enforcement responsibilities solely to copyright holders personal monitoring and detection of infringements can be largely suboptimal, considering the mass volume of contents uploaded across digital platforms per minute (Burk, 2016).

For the European Union, a central legal instrument is the Digital Services Act (DSA). Per this legislation, digital platforms are saddled with greater responsibilities to safeguard copyrighted works against infringements.

Central to the responsibilities is the integration of automated monitoring systems (Asadi, 2023). Unlike the DMCA with its 'safe harbor' principle, the DSA does not offer wide protective coverings for digital platforms. Nevertheless, the Act provides exemptions for digital platforms that act in good faith and follow content moderation procedures, balancing the need to protect the rights of IP holders with the functional aspects of managing digital platforms (Mendis, 2023). The Act has faced critics on the following grounds. First, that it stifles free expression. Secondly, 'good faith' is largely subjective to judicial interpretation. Lastly, it encourages over-blocking and censorship affecting legitimate content (Brieske, 2023).

Court actions serve as another viable means of enforcement against infringement, notwithstanding its costly and time-consuming nature. The court affords many enforcement mechanisms, a common one is the 'blocking order' - which compels internet service providers to block access to a platform hosting infringing content (Asadi, 2023). Critics hold that this method is overreaching and potentially stifles free expression (Burk, 2016).

Contributions to the conversations on whether digital platforms should be directly held liable for infringements was made in a plethora of cases. In the case of *Viacom International Inc. v. YouTube Inc.*, whether YouTube should be held liable for the infringing contents uploaded by its user was in question, the court upheld the safe harbor principle under the DMCA. A similar decision was upheld in *Tiffany (NJ) Inc. v. eBay Inc.*, where the court held that for a digital platform to be held liable, such must be in specific knowledge of the infringing acts, and not in mere general knowledge of possible infringements (Sommers and Kilaru, 2010). In addition, the court in *Lenz v. Universal Music Corp.*, held that copyright owners before giving takedown notice must

consider fair use defenses and good faith usages, as such would not be tantamount to infringements (O'Donnell, 2009).

Automated content identification systems integrated across various digital platforms is another effective means through which the copyrights of creators are protected across digital platforms. YouTube and Facebook are notable platforms that make use of sophisticated algorithms and detection technologies that remove infringing content, most times even before copyright holders physically notice them. A central concern of systems as this, as elucidated on in the preceding paragraphs is 'false positives'. Conversely, the algorithms may not detect all infringing contents. Finally, technologies required are also expensive and enforcing them might stifle the sustenance of emerging players in the digital economy (Brieske, 2023).

IV. Intermediary Liability and Private Ordering

As shown in the preceding pages of this work, digital platforms serve as intermediaries connecting users with consumers. Under certain circumstances, these intermediaries may be held responsible for the infringing activities of their users. Such circumstances can either be classified as primary or secondary liabilities (Husovec, 2019). Primary liability arises where an intermediary is actively involved in IP infringement activities, whilst secondary liability arises where intermediaries are indirectly involved in infringement activities. However, in practice, not so much distinction can be clearly made between the duo. Flowing from the foregoing, this section sets to address the question; why digital platforms face legal exposure to infringements in the first place, and the internal governance architectures that can be set in operation to manage or limit such exposure.

This focus distinguishes this section from the preceding ones, with the latter having largely focused on the IP risks affecting digital markets and the available external governance structures to limit such risks.

The position of the law on intermediary liability varies across jurisdictions. With the focus of this work placed on the US and the EU, the US legal framework exempts intermediaries from liability provided that they remove infringing contents upon the completion of a notice and take down procedure by a claimant. Conversely, the EU legal framework imposes more stringent responsibilities on intermediaries. These responsibilities are layered in different phases. The first phase comes under the EU's E-Commerce Directive 2000/31/EC, which replicated the US safe harbour's framework, where intermediaries would be free from liability if they unknowingly hosted copyright-infringing content, provided they didn't fail to act expeditiously in the instance where they are put on notice of such infringement. The second phase came under the EU's Copyright in the Digital Single Market Directive (CDSMD) of 2019. As a total departure from the first phase, large content sharing intermediaries were held directly liable for the copyright-infringing contents uploaded on their platforms and were expected to implement necessary filters that scan contents before they go live or obtain authorization from right holders, before allowing uploads from users.

The next phase, which is the current framework, was ushered in by the Digital Services Act, Regulation (EU) 2022/2065. This framework maintained the traditional safe-harbour protections but included certain obligations that vary according to the size and impact of respective platforms. The breach of these obligations may result in huge fines as high as 6% of the operator's worldwide annual turnover. These obligations are geared towards ensuring

transparency, proper risk management and the accountability of market platforms. In essence, under the DSA a very large online platform (VLOP) such as YouTube, is subjected to both the notice and action system and proactive filtering obligations.

Closely knitted to intermediary liability is the concept of private ordering, which denotes the governance frameworks of respective digital platforms set down to regulate IP enforcement. These frameworks provide quasi regulatory mechanisms for IPR holders. Instead of resorting to litigation at first instance, claimants can assess and benefit from these mechanisms, protecting their IPRs from infringements. Notable governance frameworks of certain digital platforms include Amazon's brand registry - which provides brand owners with the avenue to enroll their brand information with related IPRs and monitor infringements (Chiba, 2024); eBay's Verified Rights Owner program (VeRO program) - which allows claimants to initiate takedown procedures and protect their rights from infringements (Pilutik, 2007). Major social media and streaming platforms like YouTube, Instagram, Facebook also use sophisticated algorithms, detection technologies, and rights management tools to protect IPRs against infringements.

These governance mechanisms help provide a uniform enforcement system, notwithstanding jurisdictional boundaries, and afford the protection of IPRs in a fast and efficient fashion. Its involvement is a good translocation from court centric enforcement, which is both time and resource consuming.

V. Cross-Border Challenges and Strategic Enforcement

Enforcement of trademarks and copyright in the digital ecosystem comes with cross-border implications, creating a tension between the territorial

nature of intellectual property and the borderless architecture of digital platforms. This is reflected across various enforcement mechanisms, especially court decisions (Ryngaert, 2023). In *Google v. Equustek Solutions Inc.*, a domestic ruling was enforced on a digital platform with global reach, as the Supreme Court of Canada gave a global injunction for the removal of websites relating to the defendant from Adobe LLC's search engines worldwide, Google however refused to comply in the US, citing conflicting laws and the intermediary protection ensured the US legal system (Daskal, 2018).

Omega SA v. Costco Wholesale Corp. is another case that reflects the difficulty entailed for IP right holders to enforce their rights in the global market. The claimant sought to segment markets by selling watches which contained a copyrighted inscription at different prices in different countries and relied on copyright law to prevent unauthorized resale of the goods. However, the defendant purchased the claimant's genuine watches abroad at a lower price in an attempt to resell them domestically in the US, an act opposed by the claimant based on such resale being bereft of authorization. The defendant relied on the principle of first sale doctrine available under the US legal framework, the claimant contested this on the basis that the goods were not manufactured in the US, leaving open the question of whether domestic principles can hold sway on global goods. The US Supreme court could not extend copyright protection to prevent the resale following an equally divided decision, allowing the lower court's decision in the defendant's favor to stand, but leaving in limbo the broader issue of extraterritorial application of domestic provisions.

The foregoing developments reserve high potentials for blurred jurisdictional limits, possible forum shopping, and ongoing conflicts across competing regulatory frameworks. In addition, factors including pseudonymous accounts, false addresses, and possible cyber-attacks on digital platforms further complicate cross-border enforcement. To resolve the issues, the harmonization of IP regulations and enforcement mechanisms has for long been recommended by scholars as one viable means to address cross-border enforcement challenges (Israhadi, 2023; Bulgakova, 2023; Burk, 2010). However, the plausibility of having a global IP system is slim, considering factors such as state sovereignty, the territorial nature of IPRs, and the variance in IP enforcement structures between developed and developing worlds.

A more practical consideration for rights holders operating globally is to adopt hybrid enforcement strategies encompassing the use of platform governance mechanisms, detection and monitoring technologies, and contractual instruments. In practice such hybrid strategy would operate across many complementary levels. For instance, to bolster platform governance, right holders can enroll in cross jurisdictional IP protection programs such as the eBay's VeRO programme, ensuring protecting across all major markets where their IP is commercially active and not merely in their country of incorporation. In addition, AI tools such as Corsearch and MarkMonitor can be deployed to conduct continuous infringement tests and surveillance across platforms. Then right holders can likewise rely on the monitoring obligations enforced on large platforms under regulatory frameworks such as the DSA. Finally, licensing agreements should also incorporate clauses that anticipate infringements, affording necessary protection to right holders.

VI. Conclusion

Digital platforms have revolutionized IP enforcement in the digital ecosystem, their functions transcend serving as mere intermediaries connecting creators to consumers and now extends to the provision of regulatory governance tools, protecting against infringements and providing enforcement outcomes in the fastest and most cost-effective manner. This development presents a novel perspective and approach, for right holders and IP practitioners representing IPR holders.

For IPR holders and IP practitioners, effective protection now includes understanding the platform governance structures of respective intermediaries and adopting a hybrid approach incorporating notice and take down procedures, contractual systems, extant legal mechanisms, detection, and monitoring technologies. This way, IP practitioners can effectively advise creators on the available means to ensure IPR protection in the rapidly evolving digital ecosystem.

Looking ahead, several developments are likely to shape the trajectory of IP enforcement in the digital economy. First, the continued expansion of AI-generated content will place new pressure on existing authorship and originality doctrines, requiring courts and legislators to revisit foundational copyright principles. Second, the proliferation of AI monitoring tools raises unresolved questions of legal accountability for automated enforcement errors, which this article has identified as a gap requiring regulatory attention. Third, the tension between trademark territoriality and the borderless architecture of digital platforms will not resolve itself without either greater

international harmonization or the development of more sophisticated private ordering mechanisms capable of operating across jurisdictions.

Fourth, the licensing governance of digital platforms will become increasingly central to enforcement strategy, as the boundary between authorized and infringing use is increasingly determined by the presence or absence of licensing arrangements rather than by judicial determination. For practitioners, this means that IP enforcement strategy must evolve from a reactive, litigation-centric model to a proactive, multi-layered approach that combines contractual structuring, platform engagement, technological monitoring, and selective use of formal legal mechanisms, calibrated to the specific IP right, platform, and jurisdiction involved.

VII. References

Adu, T.L., and Thomas, B.V. (2021). 'Knowledge of Students of the Exceptions and Limitations Clause in Copyright Administration in Academic Libraries in Ghana.' *Journal of Librarianship and Information Science*, 54(4), 737-750

Alhiniti, Y., and Amro, D.H. (2025). 'Digital Trademarks (Domain Names) Protection: A Legal and Practical Analysis', in *Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives*. Cham: Springer Nature Switzerland, pp. 2793-2807.

Asadi, F. (2023). 'Digital Platforms and Intellectual Property Infringement: Exploring Legal Liability for User-Generated Content in the Context of Digital Media.' *Legal Studies in Digital Age*, 2(1), 39-50.

Bosher, H., and Yesiloglu, S. (2018). 'An Analysis of the Fundamental Tensions Between Copyright and Social Media: The Legal Implications of Sharing Images on Instagram.' *International Review of Law Computers & Technology*, 33(2), 164-186.

Brieske, J. (2023). 'Digital User Rights and Their Enforcement: What Is the Copyright Directive Asking For?' *The Journal of World Intellectual Property*, 27(1), 27-43

Bulgakova, D. (2023). 'The Liability of Online Intermediaries Under European Union Law.' *Kyiv-Mohyla Law and Politics Journal*, (8-9), 1-43.

Burk, D.L. (2010). 'Authorization and Governance in Virtual Worlds.' *First Monday*, 15(5).

Burk, D.L. (2016). 'Copyright, Culture, and Community in Virtual Worlds'. *Laws*, 5(4), 40.

Chiba, L. (2024). *Amazon Brand Registry: Why SA Brand Owners should enroll their Brands* (Spoor Gateway) 15 August, Available at: <https://spoor.com/amazon/> (Accessed 20 January 2026).

Costco Wholesale Corp., v. Omega, S.A., 562 U.S. 40 (2010).

Daskal, J. (2018). 'Google Inc. v. Equustek Solutions Inc'. *American Journal of International Law*, 112(4), 727-733.

Goodyear, M.P. (2025). 'Common law notice-and-takedown.' *NYU Journal of Intellectual Property & Entertainment Law*, 15(1), 107.

Husovec, M. (2019). 'Remedies First, Liability Second: Or Why We Fail to Agree on Optimal Design of Intermediary Liability?', in Giancarlo, F. (ed.) *The*

Oxford Handbook of Online Intermediary Liability. Oxford: Oxford University Press.

International Trademark Association. (2021) *Trademark Registration* 1 April, Available at: <https://www.inta.org/fact-sheets/trademark-registration/> (Accessed 20 January 2026).

Israhadi, E.I. (2023). 'The Impact of Developments in Artificial Intelligence on Copyright and Other Intellectual Property Laws.' *Journal of Law and Sustainable Development*, 11(11), e1965.

Jacques, S. (2024) 'Platforms and copyright in creative industries: A tool for inclusivity?', in *Research Handbook on Intellectual Property Rights and Inclusivity*. Edward Elgar Publishing, pp. 362-381.

Katz, E. (2025). *eBay VeRo: the drop shippers guide to avoiding violation* (YABALLE) 5 March, Available at: <https://yaballe.com/blog/ebay-vero-the-dropshippers-guide-to-avoiding-violations/#:~:text=What%20is%20the%20eBay%20VeRO,that%20closely%20resemble%20the%20original> (Accessed 20 January 2026).

Levin, D., and Keenan, L. (2025). *MF DOOM's company sure TEMU alleging counterfeit merchandise* (Straight Arrow News) 12 April, Available at: <https://san.com/cc/mf-dooms-company-sues-temu-alleging-counterfeit-merchandise/> (Accessed 20 January 2026).

Mendis, S. (2023). 'Copyright Enforcement on Social Media Platforms: Implications for Freedom of Expression in the Digital Public Sphere.' 463-479. https://doi.org/10.1007/978-3-031-45304-5_29

O'Donnell, K. (2009). 'Lenz v. Universal Music Corp. And the Potential Effect of Fair Use Analysis Under the Takedown Procedures of S.512 of the DMCA.' *Duke Law & Technology Review*, 1-13.

Pilutik, S. (2007). 'eBay's secondary trademark liability problem and its VeRO program.' *Bright Ideas*, 16(1).

Pryzgoda, A. (2019). 'The International Registration of Trade Marks under the Madrid System: Advantages and Disadvantages.' *Eastern European Journal of Transnational Relations*, 3(1), 67-79

Ryngaert, C. (2023). 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts'. *German Law Journal*, 24(3), 537-550.

Soltani, G. (2025). 'The Role of Artificial Intelligence in Trademark Law: Challenges and Opportunities'. *COJ Robotics & Artificial Intelligence*, 4(3).

Sommers, M., and Kilaru, N. (2010). *The Second Circuit's Decision in Tiffany v. eBay* (Finnegan) Available at: <https://www.finnegan.com/en/insights/articles/the-second-circuit-s-decision-in-tiffany-v-ebay.html> (Accessed 20 January 2026).

Tillman, J. (2020). *Romag Fasteners v. Fossil: Willful Infringement is Not Required to Recover an Award of Profits in Trademark Infringement* (Shutts) Available at: <https://www.shutts.com/business-and-legal-insights/romag-fasteners-v-fossil-willful-infringement-is> (Accessed 20 January 20

TRADE SECRETS AS THE CORE PROTECTION OF INNOVATION: RETHINKING INNOVATION PROTECTION IN AI-DRIVEN DIGITAL MARKETS

Stephanie Nma Modilim

Abstract

This article examines how artificial intelligence (AI), platform-based business models, and data-driven technologies are reshaping global markets and placing mounting structural pressure on traditional intellectual property (IP) frameworks. Although patents, copyrights, and trademarks remain the formal center of IP governance, innovation in the contemporary digital economy is increasingly protected through secrecy-based mechanisms rather than registration-centered rights. This article argues that trade secrecy operates as the functional backbone of innovation protection in AI-driven digital markets. This means that it has become the primary and most consistently used mechanism through which firms protect the technical and organizational knowledge that generates competitive value, even though patent and copyright regimes continue to receive disproportionate legal and policy attention. This claim is advanced as a reasoned inference from firm behavior, doctrinal analysis, and available indirect evidence, including patent-secrecy substitution studies and trade secret litigation patterns, rather than as an empirically settled proposition, and the article identifies the data that would be needed to test it more directly.

Drawing on comparative legal analysis, doctrinal review, and engagement with the economics and governance literature on secrecy and disclosure, the article examines why firms rely on secrecy to protect algorithms, training data, model architectures, and operational processes, and how this reliance reflects rational responses to disclosure risk, patent uncertainty, and rapid technological iteration. It defines trade secrecy against the divergent legal standards of the United States, the European Union, and the World Trade Organization's TRIPS Agreement, and analyzes how territorially bounded IP regimes struggle to govern innovation that is developed, deployed, and exploited across borders through cloud infrastructure and platform

ecosystems, illustrated through the Waymo v. Uber litigation. The article also engages directly with the principal objections to expansive trade secret protection, including concerns about innovation spillovers, algorithmic accountability, and whistleblower protection, and proposes a recalibrated governance framework that specifies the institutional mechanisms, evidentiary reforms, and trade-law integration needed to align IP law with contemporary innovation practice, in service of sustaining investment, competition, and trust in global digital markets.

I. Introduction

The digital economy has fundamentally altered how innovation is created, protected, and commercialized. Technologies such as artificial intelligence (AI), algorithmic systems, and data-driven platforms operate through continuous iteration, rapid deployment, and cross-border scalability (World Intellectual Property Organization [WIPO], 2023). Unlike traditional industrial innovation, which often culminated in discrete, identifiable inventions, innovation in AI-driven markets is process-based, cumulative, and deeply embedded in proprietary technical and organizational knowledge. Despite this transformation, intellectual property (IP) law remains largely anchored in territorial, registration-based frameworks designed for slower and more linear modes of innovation.

This misalignment between innovation practice and legal protection mechanisms has significant consequences. Patent and copyright systems continue to dominate IP discourse and policy, yet they frequently fail to capture the assets that generate the greatest economic value in the digital economy (Organization for Economic Co-operation and Development [OECD], 2019). Disclosure requirements, uncertainty surrounding patent eligibility for algorithms, and the difficulty of defining authorship in AI-generated outputs have led many firms to reassess the costs and benefits of formal IP protection. This reassessment is not merely anecdotal: empirical work on the choice between patenting and secrecy shows that firms respond to changes in disclosure obligations by shifting the mix of protection strategies they use, patenting less and relying more on secrecy when

disclosure risks jeopardize disruptive innovation (Boot & Vladimirov, 2025). In response, innovation protection has increasingly shifted toward secrecy-based mechanisms that prioritize speed, flexibility, and control over disclosure.

This article argues that secrecy-based protection has become the functional backbone of innovation governance in AI-driven digital markets, even as IP law and policy continue to marginalize its role. Rather than treating trade secrecy as a residual or supplementary form of protection, this article situates it as the primary mechanism through which firms safeguard algorithms, data, and proprietary processes. This is advanced as an inference grounded in doctrinal analysis and the available indirect evidence rather than as a claim that has been directly measured against comprehensive litigation or industry-practice data; Section IV addresses this limitation and what would be needed to test the claim more rigorously. By defining trade secrecy against its divergent jurisdictional standards, examining the structural limits of territorial IP regimes, engaging with the principal objections to expansive secrecy-based protection, and analyzing the realities of cross-border digital innovation, the article advances a recalibrated governance framework that aligns intellectual property law with contemporary innovation practices. Such alignment is essential not only for protecting innovation, but also for fostering investment, competition, and trust in global digital markets.

II. Defining Trade Secrecy And Jurisdictional Variation

Before evaluating the role of secrecy-based protection in AI-driven markets, it is necessary to define the terms this article uses. ‘Trade secret,’ ‘confidential information,’ and ‘proprietary knowledge’ are frequently used interchangeably in commentary on digital innovation, but they are not legally synonymous. This article uses ‘trade secret’ in its formal legal sense: information that derives independent economic value from not being generally known, and that is the subject of reasonable efforts to maintain its secrecy. ‘Confidential information’ and ‘proprietary knowledge’ are used only as descriptive, non-legal terms for the broader category of undisclosed

technical and business information, some of which may or may not meet the legal threshold for trade secret status in each jurisdiction. This distinction matters because the legal standards for what counts as a protectable trade secret vary meaningfully across the jurisdictions this article discusses. WIPO's (2019) comparative survey of trade secret law reaches a similar conclusion, observing that although the great majority of jurisdictions now recognize some form of trade secret protection, the scope of protectable subject matter and the conduct required to maintain it differ enough across national laws that firms operating internationally cannot safely assume a single compliance standard will satisfy every jurisdiction in which they hold confidential information.

In the United States, the Defend Trade Secrets Act of 2016 (DTSA) defines a trade secret as information for which the owner has taken 'reasonable measures' to keep it secret and which derives independent economic value from not being generally known or readily ascertainable (Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(3)). The DTSA created a federal civil cause of action layered atop the pre-existing state-law framework of the Uniform Trade Secrets Act, and empirical analysis of its first year of litigation found that the paradigm case remains a former employee who leaves with proprietary information, a pattern directly relevant to the labor-mobility and cross-border employment dynamics discussed in Section V (Levine & Seaman, 2018).

The European Union's Trade Secrets Directive uses a similar but textually distinct standard, requiring that the information be subject to 'reasonable steps' by the person lawfully in control of it to keep it secret (European Parliament and Council, 2016). While 'reasonable measures' and 'reasonable steps' are often treated as functionally equivalent in practice, courts in different EU member states and U.S. jurisdictions have not converged on identical evidentiary expectations for what qualifies as adequate protective conduct, particularly regarding cloud-based storage, access logging, and third-party vendor arrangements common in AI development.

At the multilateral level, Article 39 of the TRIPS Agreement sets a minimum international standard, requiring member states to protect undisclosed information that is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret, while also imposing a distinct obligation to protect regulatory test data submitted for pharmaceutical and agricultural chemical approval against unfair commercial use (World Trade Organization, 1994). TRIPS Article 39 establishes only a floor; individual member states retain discretion over enforcement mechanisms, remedies, and evidentiary procedure, which is precisely the source of the jurisdictional fragmentation examined in Section V.

This definitional and jurisdictional variation is not a peripheral technicality for a paper proposing cross-border governance reform. A firm operating simultaneously in the United States, the European Union, and jurisdictions that have adopted TRIPS-consistent but otherwise divergent domestic trade secret statutes faces materially different evidentiary burdens for the same underlying conduct. Section VIII returns to this variation directly, proposing mechanisms that do not require full substantive harmonization but that reduce the practical costs this variation imposes on firms and courts.

III. Innovation In Ai-Driven Digital Markets

Innovation in AI-driven digital markets differs fundamentally from the paradigms that shaped modern IP law. Rather than producing static inventions, firms are engaging in continuous cycles of development involving data collection, model training, algorithmic refinement, and deployment optimization (WIPO, 2023). These processes are often distributed across jurisdictions, relying on cloud infrastructure, remote development teams, and platform ecosystems. As a result, the value of innovation lies less in any single output and more in the accumulation of tacit knowledge, technical workflows, and non-public operational insights.

This form of innovation challenges the assumptions underlying patent and copyright protection. Patent regimes presuppose that inventions can be clearly delineated, disclosed, and examined within a reasonable timeframe. In AI contexts, however, disclosure risks revealing sensitive technical

information that may erode competitive advantage, while examination timelines frequently exceed the commercial lifespan of the technology. Copyright law, while offering protection for software code, provides limited coverage for functionality, logic, training data, or model architecture. These gaps leave significant components of digital innovation outside the effective reach of formal IP protection, a point the WIPO (2023) has itself acknowledged in surveying how AI strains existing IP categories.

Consequently, firms operating in AI-driven markets increasingly rely on internal governance mechanisms to protect innovation. Confidentiality agreements, access controls, technical safeguards, and organizational practices play a central role in preserving exclusivity. This reliance reflects rational economic behavior rather than regulatory evasion. As Friedman, Landes, and Posner (1991) observed in one of the earliest systematic economic treatments of trade secret law, secrecy and patenting function as substitute, and sometimes complementary, appropriability mechanisms, and firms select between them based on the relative costs of disclosure and detection. This article's characterization of secrecy as a primary rather than residual protection mechanism is consistent with Lemley's (2008) broader doctrinal argument that trade secrets should be understood as genuine property-like IP rights rather than as a mere gap-filler that operates only where patent or copyright protection is unavailable. Firms in AI-driven markets seek protection mechanisms that align with the speed, scale, and uncertainty inherent in digital innovation. Understanding this shift is critical to evaluating the adequacy of existing IP frameworks and identifying pathways for legal adaptation.

IV. Secrecy-Based Protection As A Central Mechanism Of Innovation Protection

Secrecy-based protection now underpins much of the value creation in AI-driven digital markets. Proprietary datasets, training methodologies, model weights, feature engineering techniques, and deployment pipelines derive economic value precisely because they remain undisclosed. These assets are not peripheral to innovation; in practice, firms increasingly treat secrecy

not as a fallback option, but as a deliberate and primary strategy for safeguarding competitive advantage.

Several factors explain this shift. Uncertainty regarding the patentability of algorithms and AI-related processes discourages reliance on patent systems. Disclosure requirements pose significant risks in fast-moving markets where competitors can rapidly replicate disclosed techniques. Empirical research on firm-level patenting behavior supports this account. Png (2017) found that the passage of the Uniform Trade Secrets Act across U.S. states was associated with increased research and development spending among larger, high-technology firms, suggesting that stronger secrecy protection encourages investment in the kind of process-based innovation characteristic of AI development. Similarly, Contigiani, Hsu, and Barankay (2018) found that heightened, employer-friendly trade secrecy protection under the inevitable disclosure doctrine is associated with reduced employee mobility and altered innovation outcomes, indicating that secrecy regimes have real, measurable effects on how firms and workers behave, not merely on how they describe their protection strategy. The doctrine Contigiani et al. study empirically originates in a decided appellate case, not merely a theoretical construct: in *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995), the Seventh Circuit affirmed a preliminary injunction barring a former PepsiCo executive from assuming a comparable role at a direct competitor, reasoning that his new position would inevitably require him to draw on PepsiCo's confidential strategic plans regardless of his subjective intentions. *PepsiCo v. Redmond* remains the doctrinal anchor for the labor-mobility dynamics this article discusses, and it illustrates concretely how courts translate a firm's abstract interest in secrecy into a concrete restraint on an individual's freedom to work for a competitor, the very tension this article's governance framework in Section VIII must accommodate. Most directly, Boot and Vladimirov (2025) provide empirical evidence, using a text-based index of trade secrecy reliance drawn from firms' own disclosures, that firms pursuing disruptive innovation increase their reliance on secrecy as patent-related disclosure obligations become more burdensome. Additionally, the global nature of digital exploitation complicates enforcement, as innovations may be deployed simultaneously across

multiple jurisdictions. Secrecy-based protection offers firms greater control over dissemination and use, enabling rapid scaling without regulatory delay. The rise of generative AI intensifies this dynamic further: Levine (2023) argues that generative AI systems complicate trade secret doctrine on both sides of the misappropriation inquiry, since the training data and model weights firms seek to protect as secrets are simultaneously at risk of being ingested, memorized, and inadvertently reproduced by other generative systems in ways existing misappropriation doctrine did not anticipate. Courts have already begun to confront the doctrinal question this raises, namely whether automated, large-scale acquisition of data qualifies as an "improper means" of misappropriation even where the underlying individual data points are publicly accessible. In *Compulife Software, Inc. v. Newman*, 959 F.3d 1288 (11th Cir. 2020), the Eleventh Circuit held that a competitor's use of an automated bot to scrape more than 42 million individually public insurance quotes from the plaintiff's website could constitute misappropriation by improper means, reasoning that a bot's capacity to compile a protected database at a scale and speed no human could replicate distinguishes automated extraction from ordinary, permissible access. *Compulife* is directly relevant to the generative AI context Levine describes: it suggests that a firm's trade secret protection may survive the public accessibility of individual data points scraped or ingested by an AI system, while leaving open exactly how much automated extraction is too much, a line-drawing problem this article's proposed evidentiary and procedural coordination in Section VIII is intended to help courts and firms navigate more predictably.

It is important to be precise about what this evidence does and does not establish. The studies cited above measure the relationship between secrecy law and firm behavior in general, and in some cases in AI-adjacent technology sectors specifically, but no dataset currently tracks the relative frequency of trade secret reliance against patent or copyright protection specifically within AI firms, nor systematically compares AI trade secret litigation rates and outcomes across jurisdictions. Levine and Seaman's (2018) empirical study of DTSA litigation, while foundational, was limited to the statute's first year and was not sector specific. The claim advanced in this article, that trade secrecy functions as the primary protective mechanism

in AI-driven markets, should therefore be understood as a reasoned inference from firm-level economic behavior, doctrinal structure, and adjacent empirical literature, rather than as a proposition that has been directly and comprehensively measured. A firm-level survey of AI companies' protection strategies, and a systematic coding of AI-related trade secret litigation comparable to Levine and Seaman's DTSA study, would substantially strengthen the empirical foundation for this claim, and the article returns to this point in the Conclusion as a direction for future research.

This reliance also exposes structural weaknesses in existing legal regimes. Trade secrecy protections remain largely national in scope, with significant variation in substantive standards, evidentiary thresholds, and remedies, as detailed in Section II. As innovation scales across borders, the territorial limits of secrecy-based regimes become increasingly pronounced. Misappropriation risks rise, enforcement becomes fragmented, and legal uncertainty undermines investment and collaboration. These challenges underscore the need to reassess how secrecy-based protection is situated within IP governance; a need this article develops in Sections V through VIII.

V. Limitations Of Territorial Ip And Enforcement Models

Territorial IP regimes struggle to govern innovation that transcends national boundaries. Secrecy-based assets move fluidly through cloud infrastructure, cross-border development teams, and platform ecosystems, making misappropriation difficult to detect and prove. Traditional evidentiary standards, designed for physical documents and localized theft, are ill-suited to digital environments characterized by distributed access and instantaneous duplication.

The litigation between Waymo LLC and Uber Technologies, Inc. illustrates these dynamics concretely. Waymo, the autonomous vehicle unit of Google's parent company Alphabet, sued Uber in 2017, alleging that a former Waymo engineer, Anthony Levandowski, downloaded approximately 14,000 confidential files related to Waymo's LiDAR (light detection and ranging) technology before leaving to found a self-driving truck startup that Uber

subsequently acquired (Butzel Long, 2018; Harvard Journal of Law & Technology, 2018). The case was framed as both a trade secret misappropriation claims under the DTSA and California's Uniform Trade Secrets Act and, initially, a patent infringement claim, though the patent claims were later dropped, leaving the dispute to be resolved almost entirely on secrecy-based grounds. The parties settled after only four days of trial for approximately \$245 million in Uber equity, before a jury verdict or appellate ruling could clarify several unresolved evidentiary questions, including how much of the trial record needed to remain under seal to protect the trade secrets at issue and how digital forensic evidence, such as file-download logs and device metadata, should be weighed in proving misappropriation in a cloud-based, cross-employer environment. The dispute demonstrates both the commercial stakes attached to AI-relevant secrecy-based assets and the practical difficulty of adjudicating misappropriation claims where the underlying technology is embedded in code, sensor data, and engineering know-how rather than in a discrete, physically identifiable object. Although the civil dispute between Waymo and Uber settled short of a verdict, the underlying conduct did produce a fully adjudicated outcome through a parallel criminal prosecution. Levandowski was separately indicted on 33 federal counts of trade secret theft and attempted theft under the Economic Espionage Act, 18 U.S.C. § 1832; he pleaded guilty to one count in March 2020, and in August 2020 Judge William Alsup of the U.S. District Court for the Northern District of California sentenced him to eighteen months in prison, a \$95,000 fine, and restitution of \$756,499.22 to Waymo, describing the theft as the largest trade secret crime he had encountered on the bench (United States v. Levandowski, No. 3:19-cr-00377 (N.D. Cal. 2020)). The criminal case establishes, as a matter of adjudicated fact rather than settled allegation, that at least one internal Waymo document, the "Chauffeur Weekly Update," constituted a protectable trade secret, and it demonstrates that criminal enforcement under the Economic Espionage Act can operate as a real, resolved backstop where civil litigation between corporate parties settles before trial produces a binding ruling. A separate dispute did proceed through a full civil jury trial and appellate review on facts closely analogous to Waymo's, and it illustrates both the evidentiary role of digital access records and the scale of the stakes involved. In Epic Systems Corp. v. Tata

Consultancy Services Ltd., 980 F.3d 1117 (7th Cir. 2020), a Wisconsin jury found that TCS, an India-based information technology firm, had misappropriated Epic's healthcare-software trade secrets after a TCS employee used improper credentials to download thousands of documents from Epic's confidential client web portal over a two-year period, evidence that was itself proven through the same kind of file-access logs and download records that remained contested and unresolved in the settled Waymo litigation. The jury initially awarded Epic \$940 million in combined compensatory and punitive damages; the district court and, on appeal, the Seventh Circuit substantially reduced the punitive component on constitutional due-process grounds, leaving a final judgment of approximately \$280 million. *Epic v. TCS* thus supplies what Waymo could not: a fully litigated resolution confirming that digital access logs can establish trade secret misappropriation to a jury's satisfaction, while its facts, an offshore contractor accessing a U.S. firm's confidential systems, also reinforce this article's point in Section V that cross-border enforcement is a live, recurring problem rather than a hypothetical one.

Enforcement challenges are further compounded by labor mobility and outsourcing practices common in digital industries. Employees and contractors often operate across jurisdictions, increasing the risk of inadvertent disclosure or intentional misappropriation, a dynamic Levine and Seaman (2018) found to be the dominant fact pattern in DTSA litigation generally. Once proprietary information crosses borders, remedies become uncertain, and jurisdictional fragmentation weakens deterrence. These gaps undermine the protective function of secrecy-based regimes and erode confidence in IP systems. The extent and limits of cross-border enforcement have, in fact, now been tested to a full decided judgment. In *Motorola Solutions, Inc. v. Hytera Communications Corp.*, 108 F.4th 458 (7th Cir. 2024), engineers who had been recruited away from Motorola's Malaysian office downloaded thousands of files containing Motorola's trade secrets and used them to help Hytera, a Chinese manufacturer, develop a competing line of radios; a jury found DTSA and copyright violations and, after post-trial proceedings, awarded Motorola approximately \$407 million in trade secret damages, entirely for conduct and sales that occurred outside the United

States. The Seventh Circuit affirmed that the DTSA applies extraterritorially where an "act in furtherance" of the misappropriation, such as marketing the infringing products at a U.S. trade show, occurred domestically, allowing recovery based on the defendant's worldwide sales. *Motorola v. Hytera* is directly relevant to the governance proposals in Section VIII: it shows that at least one U.S. court has already been willing to extend domestic trade secret law to reach wholly foreign misappropriation, without waiting for the treaty-level coordination this article proposes, but it does so through an ad hoc statutory interpretation rather than a coordinated evidentiary or procedural framework, and Hytera's subsequent refusal to comply with the resulting judgment illustrates the practical enforcement limits that remain even after a favorable, fully litigated ruling.

The economic implications become significant. Firms face heightened risks when scaling globally, while investors discount valuations to account for weak cross-border protection. Regulatory arbitrage and over-reliance on private ordering, discussed in Section VI, become rational responses to fragmented enforcement. Without coordinated legal adaptation, territorial IP models will continue to lag the realities of digital innovation.

VI. Platform Markets And Private Ordering

In response to enforcement limitations, platform governance and contractual controls increasingly regulate innovation protection. Licensing agreements, access restrictions, and technical interoperability standards function as de facto substitutes for statutory IP protection. Dominant platforms shape the conditions under which proprietary information is shared, used, or monetized, effectively acting as private regulators of innovation. Cohen (2017) describes this phenomenon as platforms assuming quasi-regulatory functions over the digital economy, mediating access to infrastructure, data, and markets in ways that formal law neither anticipates nor fully constrains. In later work, Cohen (2019) extends this analysis to argue that platforms exercise a form of infrastructural power that operates independently of, and sometimes in tension with, traditional public regulatory authority.

While private ordering offers efficiency and flexibility, it also raises normative concerns. Power asymmetries between platforms and smaller innovators can distort competition and limit entry. Pasquale (2015) argues that the opacity created by proprietary algorithms and data practices, much of it maintained through trade secret and contractual protection, insulates dominant firms from meaningful public or competitive scrutiny, describing a shift from ‘legitimacy-via-transparency to reassurance-via-secrecy’ in how firms justify their market power. Secrecy-based protection, when reinforced through contract and technical control, may entrench information silos and reduce spillover innovation. These dynamics highlight the risks of relying solely on private governance mechanisms to protect innovation in the digital economy, and they are developed further in Section VII, which addresses the principal objections to expansive secrecy-based protection directly.

Addressing these concerns requires situating secrecy-based protection within broader regulatory frameworks governing platforms, competition, and digital markets. Public law safeguards remain essential to ensuring that innovation protection does not come at the expense of fairness, transparency, or long-term market dynamism.

VIII. Countervailing Interests: Transparency, Competition, And The Limits Of Secrecy-Based Protection

A paper advocating for recalibrated governance of secrecy-based protection must engage seriously with the objections to expansive trade secrecy, rather than treating the case for stronger protection as self-evidently correct. Three objections are most pressing in the AI context: the risk to innovation spillovers, the tension with algorithmic accountability, and the risk to whistleblower protection.

The first objection concerns spillovers. Because trade secrets are, by definition, undisclosed, and because trade secret protection is not subject to the fixed expiration that limits patent monopolies, critics have long argued that expansive secrecy restricts the acquisition and recombination of ideas that drive cumulative innovation and may unacceptably restrict labor mobility and competition (Hettinger, 1989). This is not merely a theoretical concern;

a 2021 U.K. government-commissioned analysis of the economic and innovation impacts of trade secrets concluded that because trade secrets can theoretically last indefinitely and involve no disclosure obligation, they can reduce the research and development spillovers that would otherwise flow from disclosed, patented innovation, potentially lowering aggregate productivity growth even as they protect individual firms' returns (Gov.UK, 2021). Set against this, the OECD (2021) has argued that trade secrecy also enables forms of collaboration, such as joint ventures and licensing arrangements built on shared confidential information, that would not occur if firms had to rely solely on public disclosure. The tension between these positions is genuine and is not resolved by this article; it counsels caution against treating expanded secrecy-based protection as costless, and it is a central reason the governance framework proposed in Section VIII pairs secrecy recognition with competition-law safeguards rather than proposing secrecy protection alone.

The second objection concerns algorithmic accountability. AI systems increasingly make or inform decisions with significant consequences for individuals, including in lending, hiring, and content moderation. Trade secret protection over the algorithms and training data underlying these systems can shield them from the scrutiny needed to detect bias, error, or harm (Pasquale, 2015). Villasenor (2025) engages this tension directly, arguing that AI developers should be able to hold trade secret rights in algorithms even where the developers themselves cannot fully explain how the algorithm reaches a given output, while also acknowledging that trade secret owners must be able to describe the algorithm in sufficient detail to sustain a misappropriation claim, and that this obligation interacts with regulatory disclosure requirements. The EU's Artificial Intelligence Act reflects this tension in positive law: it requires providers of high-risk AI systems to supply clear documentation of training, validation, and testing data, and their intended purpose and accuracy metrics, obligations that regulators and commentators recognize will sometimes encroach on information firms would otherwise protect as trade secrets (Regulation (EU) 2024/1689, arts. 13, 53; Herbert Smith Freehills Kramer, 2025). This is not a peripheral compliance detail; it reflects a structural point this article's governance

framework must accommodate, namely that evidentiary and disclosure reform cannot be designed solely around firms' interest in secrecy without also addressing the public's interest in reviewing how AI systems that affect them operate.

The third objection concerns whistleblower protection. Employees who become aware of unlawful conduct, safety risks, or regulatory violations embedded in a firm's confidential systems may be deterred from reporting that conduct if doing so exposes them to trade secret liability. The DTSA itself contains a whistleblower immunity provision, protecting an individual from liability for disclosing a trade secret in confidence to a government official or attorney solely for the purpose of reporting a suspected violation of law (Defend Trade Secrets Act of 2016, 18 U.S.C. § 1833(b)). This provision demonstrates that even the strongest recent expansion of federal trade secret protection was drafted with an explicit carve-out for this concern, but the immunity is narrow, procedural, and largely untested outside the United States, and it does not resolve the underlying tension between an employee's duty of confidentiality and the public interest in disclosure of misconduct embedded in AI systems operating across borders.

Taken together, these objections do not undermine the case for recognizing secrecy-based protection as central to how AI-driven innovation is protected; the evidence reviewed in Section IV supports that recognition as a description of firm behavior. What the objections do undermine is any governance response that treats stronger, less accountable secrecy protection as an unambiguous good. This article's own analysis in Section VI, that secrecy reinforced through contract and technical control may entrench information silos, is itself an acknowledgment of this point. A defensible governance framework must therefore recognize secrecy's functional centrality while building in the competition, transparency, and whistleblower safeguards that respond to these objections. Section VIII attempts to do so.

VIII. Toward A Recalibrated Governance Framework

Reconceptualizing innovation protection requires repositioning secrecy-based regimes within IP governance through concrete institutional mechanisms, not general aspirations. Three areas of reform are addressed here: evidentiary standards, cross-border enforcement coordination, and the balance between protection and competing interests.

First, evidentiary standards must evolve to recognize digital provenance, secure audit trails, and technologically verifiable proof of misappropriation. Concretely, this means courts and rule-making bodies should recognize cryptographic timestamping and secure, tamper-evident audit logs, technologies already used in software version control and increasingly discussed as a basis for blockchain-based provenance systems, as competent evidence of when and how a given dataset, model architecture, or codebase was created and accessed. Procedural rules governing discovery should be updated to specify standards for authenticating cloud-stored access logs and device metadata across cloud service providers located in different jurisdictions, an evidentiary gap the *Waymo v. Uber* litigation exposed but did not resolve, since the case settled before trial produced a binding appellate ruling on these questions. National procedural rulemaking bodies, and, at the international level, the WIPO Standing Committee on the Law of Patents, are appropriate venues to develop model evidentiary rules that courts in multiple jurisdictions could adopt on a voluntary basis, reducing the current inconsistency in how digital provenance evidence is treated from one jurisdiction to the next.

Second, cross-border cooperation should move beyond minimal harmonization toward coordinated enforcement mechanisms tailored to digital innovation. Concretely, this could take the form of a dedicated working group within the WTO TRIPS Council, or an expanded mandate for the WIPO Standing Committee on the Law of Patents, tasked specifically with developing model rules for cross-border trade secret discovery, comparable to how the Hague Evidence Convention structures cross-border discovery in other civil litigation contexts but adapted for digital evidence. Mutual legal

assistance treaty frameworks, currently used primarily for criminal enforcement cooperation, could be extended or supplemented with a parallel civil-enforcement protocol specific to trade secret misappropriation involving cloud infrastructure or platform intermediaries located outside the forum jurisdiction. Aligning substantive standards, for instance narrowing the gap between the DTSA's 'reasonable measures' standard and the EU Directive's 'reasonable steps' standard through interpretive guidance rather than statutory amendment, would reduce fragmentation without requiring the politically difficult step of full substantive harmonization. Integrating secrecy-based protection into digital trade frameworks, addressed further in Section IX, is particularly important given the centrality of data flows and platform intermediation to contemporary innovation.

Third, governance frameworks must balance innovation protection with competition, transparency, and the whistleblower and accountability concerns detailed in Section VII. Recognizing secrecy-based protection as central does not require abandoning formal IP rights or treating secrecy as immune from public oversight. Concretely, this balance can be operationalized through procedural safeguards already familiar to courts, such as protective orders and in-camera review, extended specifically to accommodate the regulatory disclosure obligations AI providers face under frameworks like the EU AI Act, so that a firm's trade secret claim over an algorithm does not categorically override a regulator's or affected individual's ability to obtain the information needed to assess bias, safety, or legal compliance. It calls for an integrated approach that reflects how innovation is created and protected in AI-driven markets while preserving the public and competitive interests that unqualified secrecy protection would otherwise compromise.

IX. Implications For Innovation, Investment, And Global Trade

Aligning IP governance with secrecy-based innovation has significant implications for innovators, investors, and policymakers. Firms must adopt internal governance practices, such as documented access controls and audit-trail retention, that are specific enough to satisfy the 'reasonable

measures' or 'reasonable steps' thresholds described in Section II across every jurisdiction in which they operate, rather than relying on a single compliance standard designed around one legal system. Investors require clearer signals of enforceability and risk allocation. Policymakers must recognize that failure to adapt IP frameworks risks undermining confidence in innovation ecosystems.

Existing trade agreements provide a partial but incomplete foundation for this alignment. TRIPS Article 39 establishes the baseline multilateral obligation to protect undisclosed information but leaves enforcement mechanisms, evidentiary standards, and remedies to domestic implementation, which is the principal source of the fragmentation discussed throughout this article (World Trade Organization, 1994). The USMCA, which replaced NAFTA in 2020, went further than TRIPS by expanding trade secret protection and, notably, adding provisions criminalizing trade secret misappropriation, including government-affiliated or state-sponsored trade secret theft, a response to concerns about cyber-enabled economic espionage rather than the ordinary private-party misappropriation at issue in disputes like *Waymo v. Uber* (Gov.UK, 2021). The CPTPP contains parallel disciplines directed specifically at combating trade secret theft conducted through cyber intrusion, with phased implementation periods for some member states, reflecting a similar recognition that digital-era misappropriation raises distinct enforcement challenges from traditional, physical trade secret theft.

None of these agreements, however, directly address the digital-provenance evidentiary standards or platform-intermediated misappropriation scenarios described in Sections V and VIII. USMCA and CPTPP were negotiated to respond primarily to cyber-espionage and criminal misappropriation, not to the civil evidentiary and cross-border discovery challenges that dominate private trade secret litigation in AI-driven markets. This is a genuine gap and an opportunity: the next generation of digital trade agreements, or supplementary protocols to existing agreements, could extend the criminalization and cooperation provisions already present in USMCA and CPTPP to cover the civil evidentiary coordination mechanisms proposed in Section VIII, without requiring an entirely new treaty framework.

At the global level, coherent governance can promote fair competition and reduce trade distortions arising from uneven protection. This does not mean that uniformly stronger secrecy-based protection is appropriate for every jurisdiction regardless of its stage of development: Kim, Lee, Park, and Choo (2012) find that the growth-enhancing effect of stronger IP protection is contingent on a country's level of economic and technological development, with weaker protection sometimes better serving imitation-driven growth in developing economies. The governance recalibration proposed here is accordingly framed as a floor of procedural and evidentiary coordination among major AI-producing jurisdictions, not a template for uniform substantive strengthening across all WTO members. By aligning legal frameworks with market realities, and by building the specific institutional mechanisms described above into existing trade-law infrastructure rather than proposing an entirely new regime, states can foster sustainable innovation while preserving trust in IP systems.

X. Conclusion

The digital economy has transformed the nature of innovation, rendering traditional IP paradigms increasingly inadequate on their own. While patents and copyrights remain formally central to IP doctrine, this article has argued that secrecy-based protection functions as the primary mechanism through which firms protect the algorithms, data, and organizational knowledge that generate competitive value in AI-driven digital markets. This argument is supported by doctrinal analysis of the structural mismatch between patent and copyright regimes and the realities of AI development, by economic literature on firms' patent-secrecy substitution behavior, and by the Waymo v. Uber litigation as a concrete illustration of how these dynamics play out in practice, but it is advanced as an evidence-based inference rather than as a directly measured empirical finding, a limitation this article has tried to state plainly rather than obscure.

The article's contribution, situated against the existing literature, is threefold. First, it connects doctrinal IP scholarship on trade secrecy to the economics literature on patent-secrecy substitution and the platform-governance

literature on private ordering, three bodies of scholarship that are frequently cited separately but rarely integrated around the specific problem of AI-driven innovation protection. Second, it takes seriously, rather than sets aside, the countervailing objections to expansive secrecy-based protection, particularly the tension between trade secrecy and algorithmic accountability that is becoming acute as AI regulation, exemplified by the EU AI Act, imposes disclosure obligations that intersect directly with firms' secrecy interests. Third, it translates the general call for 'recalibrated governance' into specific institutional proposals, identifying candidate venues (the WIPO Standing Committee on the Law of Patents, the WTO TRIPS Council, extended mutual legal assistance frameworks) and concrete evidentiary mechanisms (cryptographic timestamping, secure audit logs, protective-order protocols tied to regulatory disclosure obligations) rather than leaving the governance proposal at the level of general principle.

This analysis has clear limitations. It relies on secondary and indirect empirical literature rather than original data collection; it uses a single case study, chosen for its prominence and its illustration of the evidentiary issues addressed in Section VIII, rather than a systematic sample of AI-related trade secret disputes; and its comparative legal analysis is limited to the United States, the European Union, and the TRIPS baseline, rather than a comprehensive survey of trade secret regimes across all jurisdictions relevant to global AI development, including major AI markets in Asia. These limitations point directly to productive future research: a systematic, sector-specific empirical study of AI firms' reliance on trade secrecy relative to patenting, comparable in method to Levine and Seaman's (2018) DTSA litigation study but focused specifically on AI-related disputes; a comparative doctrinal survey extending beyond the U.S.-EU-TRIPS framework used here to major Asian AI markets; and empirical research on how platform contract terms, of the kind discussed in Section VI, actually allocate trade secret risk between dominant platforms and smaller innovators in practice.

Such recalibration, pursued with the specificity and the acknowledgment of countervailing interests this article has tried to model, is essential to ensuring

that intellectual property law continues to promote innovation, investment, and economic growth in a rapidly evolving global landscape.

XI. References

Boot, A., & Vladimirov, V. (2025). Disclosure, patenting, and trade secrecy. *Journal of Accounting Research*, 63(1), 5–56. <https://doi.org/10.1111/1475-679X.12580>

Butzel Long. (2018, February 9). Waymo v. Uber — “Epic” trade secret case involving autonomous vehicles settles for \$244 million. <https://www.butzel.com/alert-Waymo-v-Uber-Epic-Trade-Secret-Case-Involving-Autonomous-Vehicles-Settles-for-244-Million>

Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, 51(1), 133–204.

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership, ch. 18 (2018).

Compulife Software, Inc. v. Newman, 959 F.3d 1288 (11th Cir. 2020).

Contigiani, A., Hsu, D. H., & Barankay, I. (2018). Trade secrets and innovation: Evidence from the “inevitable disclosure” doctrine. *Strategic Management Journal*, 39(11), 2921–2942. <https://doi.org/10.1002/smj.2941>

Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836 (2016).

Epic Systems Corp. v. Tata Consultancy Services Ltd., 980 F.3d 1117 (7th Cir. 2020).

European Parliament and Council. (2016). Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Friedman, D. D., Landes, W. M., & Posner, R. A. (1991). Some economics of trade secret law. *Journal of Economic Perspectives*, 5(1), 61–72. <https://doi.org/10.1257/jep.5.1.61>

Gov.UK. (2021). The economic and innovation impacts of trade secrets. Intellectual Property Office. <https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets>

Harvard Journal of Law & Technology Digest. (2018, March 3). Waymo v. Uber: Surprise settlement five days into trial. <https://jolt.law.harvard.edu/digest/waymo-v-uber-surprise-settlement-five-days-into-trial>

Herbert Smith Freehills Kramer. (2025, November 6). Trade secrets in the AI era: Navigating transparency under the EU AI Act. <https://www.hsfkramer.com/insights/2025-10/trade-secrets-in-the-ai-era-navigating-transparency-under-the-eu-ai-act>

Hettinger, E. C. (1989). Justifying intellectual property. *Philosophy & Public Affairs*, 18(1), 31–52.

Kim, Y. K., Lee, K., Park, W. G., & Choo, K. (2012). Appropriate intellectual property protection and economic growth in countries at different levels of development. *Research Policy*, 41(2), 358–375. <https://doi.org/10.1016/j.respol.2011.09.003>

Lemley, M. A. (2008). The surprising virtues of treating trade secrets as IP rights. *Stanford Law Review*, 61(2), 311–353.

Levine, D. S. (2023). Generative artificial intelligence and trade secrecy. *Journal of Free Speech Law*, 3(2), 559–580.

Levine, D. S., & Seaman, C. B. (2018). The DTSA at one: An empirical study of the first year of litigation under the Defend Trade Secrets Act. *Wake Forest Law Review*, 53, 105–177.

Motorola Solutions, Inc. v. Hytera Communications Corp., 108 F.4th 458 (7th Cir. 2024).

Organization for Economic Co-operation and Development. (2019). *Protecting and promoting innovation in the digital economy*. OECD Publishing.

Organization for Economic Co-operation and Development. (2021). *Trade secrets, innovation, and economic competitiveness*. OECD Publishing.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995).

Png, I. P. L. (2017). Secrecy and patents: Theory and evidence from the Uniform Trade Secrets Act. *Strategy Science*, 2(3), 176–193. <https://doi.org/10.1287/stsc.2017.0035>

JOURNAL OF IP PROFESSIONALS

United States-Mexico-Canada Agreement, ch. 20 (2020).

United States v. Levandowski, No. 3:19-cr-00377 (N.D. Cal. 2020) (judgment entered Aug. 4, 2020).

Villasenor, J. (2025). Artificial intelligence, trade secrecy, and the challenge of transparency. *North Carolina Journal of Law & Technology*, 25(3), 495–540.

Waymo LLC v. Uber Technologies, Inc., No. 3:17-cv-00939 (N.D. Cal. filed Feb. 23, 2017) (settled Feb. 9, 2018).

World Intellectual Property Organization. (2019). *Trade secrets and innovation*. WIPO Publishing.

World Intellectual Property Organization. (2023). Intellectual property and artificial intelligence. WIPO Publishing.

World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).



BEYOND COMPLIANCE: DESIGNING HUMAN-CENTERED AI GOVERNANCE FRAMEWORKS FOR THE CREATIVE AND CULTURAL INDUSTRIES

Onyinye Odita

Abstract

The rapid integration of generative artificial intelligence into the creative and cultural industries has exposed significant limitations in existing, compliance-oriented regulatory frameworks. While current responses to AI governance largely focus on formal legal rules and risk containment, they often fail to address deeper concerns relating to human creativity, cultural diversity, creative labour, and social welfare. This article argues for a shift from rule-based compliance toward a human-centered, values-driven AI governance framework tailored to the unique dynamics of the creative and cultural sectors. Drawing on international normative instruments such as the UNESCO Recommendation on the Ethics of AI, the OECD AI Principles, WIPO's Conversations on AI and Intellectual Property, and comparative regional approaches including the EU AI Act, the UK, US, and Global South perspectives, the article examines how law and policy can better safeguard creative agency and cultural autonomy. It further analyses key governance challenges, including the erosion of human creative agency, bias and cultural homogenization, data colonialism, and power asymmetries between platforms and creators. The article proposes an integrated, multi-layered governance model that embeds human oversight, inclusivity, transparency, and sustainability into AI design and deployment. Ultimately, it contends that effective AI governance in the creative and cultural industries must move beyond minimal compliance to actively promote ethical innovation, equitable value distribution, and the long-term vitality of cultural ecosystems.

Keywords: artificial intelligence; human-centered AI governance; creative and cultural industries; intellectual property; cultural rights; data colonialism; creative labour.

Introduction

The emergence of generative artificial intelligence (AI) has produced an unprecedented disruption across intellectual property law and the wider creative economy. Although it is now widely accepted that these technologies are a durable feature of cultural production, that acceptance has not resolved the substantial legal and normative uncertainties they generate. Generative AI presents a profound dual character: it offers significant creative and economic opportunity, yet, absent careful governance, it also threatens the rights, livelihoods, and cultural autonomy of the creators on whose work it depends.

Understandably, society has not refrained from responding to issues that have been raised by AI, particularly in relation to frameworks and governance mechanisms. However, the response has to date been fragmented and uneven, and has frequently failed to take into account the diverse domains from which these issues arise (Attard-Frost et al., 2023). The result is a body of responses that, although well-intentioned, remains insufficient to address the underlying challenges.

The current regulatory framework focuses largely on the legal perspective and the rules intended to guide the activities of generative AI systems. However, the nature of the disruption demands a governance model that puts human creativity, cultural values, and social welfare at its core. This is because, beyond their effect on legal norms, the questions raised by generative AI strike at the foundations of human creativity and threaten the fabric of cultural values (UNESCO, 2022).

This article therefore argues for a holistic approach to AI governance in the creative and cultural industries—one that moves beyond a narrowly rule-based model toward a more comprehensive and organic framework capable of responding to the cultural, economic, and social dimensions of generative AI's disruption.

The argument proceeds in six parts. The first establishes the conceptual foundation, defining the creative and cultural industries, the idea of human-

centered AI governance, and the shift from compliance to values-driven regulation. The second surveys the legal and normative frameworks shaping AI governance, from international instruments to regional and domestic models, and situates the intellectual property, cultural-rights, and labour-law dimensions of the field. The third identifies the principal governance challenges confronting the sector. The fourth articulates the principles of a human-centered framework, and the fifth translates those principles into an integrated, multi-layered institutional design illustrated by concrete examples. The article concludes with a set of specific and actionable policy recommendations.

Conceptual Foundation

At the outset it is necessary to clarify what is meant by the “creative and cultural industries” (CCIs), a term used throughout this article. Following established definitions, the CCIs encompass those sectors whose principal activity is the creation, production, and commercialisation of goods and services with cultural, artistic, or heritage value—including music, film and audiovisual production, the visual arts, publishing, design, video games, performing arts, and heritage and museum work (Hesmondhalgh, 2018; UNESCO, 2009). These sectors are far from homogeneous: the governance pressures facing a streaming-dominated music market differ markedly from those facing a publicly funded heritage museum or an independent game studio. Where the analysis below turns on such differences, they are identified; otherwise, the term is used to denote the sector’s shared exposure to automated cultural production. This scoping matters because human-centered governance must remain sensitive to the distinct economic structures, labour relations, and cultural functions of each sub-sector.

Artificial intelligence has become an increasingly integral component of the creative and cultural industries, reshaping how cultural goods are produced, distributed, and consumed across sectors such as music, film, visual arts, publishing, gaming, and heritage preservation. Through tools such as generative models, recommendation algorithms, and automated content curation systems, AI now participates directly in creative processes ranging

from idea generation and composition to editing, marketing, and audience engagement, often in collaboration with human creators. This integration has blurred traditional boundaries between human authorship and machine assistance, giving rise to hybrid forms of creativity that challenge established legal, economic, and cultural assumptions. At the same time, AI's reliance on large-scale cultural data raises concerns about originality, bias, cultural homogenization, and the marginalization of minority voices, particularly within globalized digital platforms. As a conceptual foundation, understanding AI in the creative and cultural industries requires recognizing it not merely as a technical tool, but as a socio-technical system embedded within cultural, economic, and regulatory contexts, whose governance directly affects creative autonomy, cultural diversity, and the sustainability of creative labour.

Human-centered AI governance refers to an approach to the design, deployment, and regulation of artificial intelligence systems that prioritizes human dignity, agency, and societal values over purely technical efficiency or formal legal compliance. Within this framework, AI is understood as a tool that should enhance, rather than displace or undermine, human creativity, cultural expression, and social well-being. Human-centered governance emphasizes principles such as transparency, accountability, fairness, inclusiveness, and meaningful human oversight, ensuring that affected stakeholders—particularly creators, cultural workers, and communities—retain control over how AI systems influence creative processes and cultural outputs. Crucially, it situates governance beyond static rules, viewing it as an ongoing, participatory process that integrates ethical norms, rights-based protections, and contextual sensitivity to cultural diversity. As a conceptual foundation for this article, human-centered AI governance provides the normative lens through which AI's role in the creative and cultural industries is assessed, framing regulation as a mechanism for safeguarding human creativity, cultural autonomy, and equitable value distribution in an increasingly automated cultural economy.

The shift from compliance to values-driven governance reflects a critical reorientation of AI regulation away from narrow, checklist-based adherence

to legal rules toward a holistic framework grounded in normative and societal values. In the context of the creative and cultural industries, compliance-focused governance often prioritizes formal conformity with data protection, copyright, or AI safety requirements, while overlooking deeper concerns such as creative autonomy, cultural integrity, fairness in remuneration, and long-term impacts on cultural ecosystems. Values-driven governance, by contrast, embeds principles such as human dignity, cultural diversity, inclusiveness, transparency, and accountability into both the design and operation of AI systems, ensuring that governance mechanisms respond to the lived realities of creators and cultural communities. This approach treats AI governance as a continuous, adaptive process that integrates ethical reasoning, stakeholder participation, and institutional responsibility, rather than a static legal obligation. As a conceptual foundation for this article, moving beyond compliance underscores the argument that effective AI governance in the creative and cultural industries must be guided not only by what is legally permissible, but by what is culturally sustainable, socially just, and human-affirming.

Legal Frameworks Shaping Ai Governance

International Normative Instruments

UNESCO Recommendation on the Ethics of AI: By outlining a values-based, human-centered strategy based on human rights, dignity, and cultural diversity, the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) marks a historic worldwide normative framework influencing AI governance. As the first global standard-setting instrument on AI adopted by consensus of UNESCO Member States, the Recommendation has considerable persuasive authority despite not being legally binding. It also increasingly influences national legislation, policy formulation, and institutional practices. While putting special emphasis on the preservation and advancement of cultural diversity, innovation, and access to culture—issues crucial to the creative and cultural industries—it advances fundamental values including openness, accountability, fairness, privacy, human oversight, and sustainability. Notably, the Recommendation

recognizes the risks of cultural homogenization, bias, and data extraction posed by AI systems trained on dominant cultural datasets, and calls for inclusive data governance, equitable benefit-sharing, and respect for the rights of creators and cultural communities. As a legal and normative framework, UNESCO's Recommendation shapes AI governance by moving states beyond minimal compliance toward proactive, values-driven regulation that integrates ethical safeguards into AI design, deployment, and oversight, making it especially relevant for governing AI's growing influence in creative production and cultural expression.

OECD AI Principles: The OECD AI Principles (2019) constitute one of the most influential international policy frameworks shaping contemporary AI governance, providing a values-based yet implementation-oriented approach that has been widely adopted by both OECD members and non-member states. As the first intergovernmental standard on artificial intelligence, the principles promote human-centered and trustworthy AI by emphasizing inclusive growth, sustainable development, and human well-being, alongside respect for human rights, democratic values, and the rule of law. They articulate key governance pillars, including transparency and explainability, robustness and safety, accountability, and responsible stewardship across the AI lifecycle. Despite not being legally enforceable, the OECD AI Principles have a substantial normative and regulatory impact by influencing sector-specific guidelines, national AI policies, and regulatory impact assessments. This is especially true given their practical emphasis on risk management and institutional accountability. The OECD framework encourages governments and industry players to incorporate ethical values and human oversight into AI systems while balancing innovation with societal trust and cultural sustainability. This encourages a shift from merely legal compliance toward responsible innovation in shaping AI governance, including within the creative and cultural industries.

WIPO Conversation on AI and IP: The WIPO Conversation on Intellectual Property and Artificial Intelligence constitutes an important soft-law process shaping global AI governance at the intersection of technology, creativity, and intellectual property (World Intellectual Property Organization, 2019).

Initiated by the World Intellectual Property Organization as a multistakeholder dialogue rather than a treaty-making process, the Conversation brings together states, creators, technology developers, industry bodies, and civil society to examine how existing IP regimes respond to AI-generated and AI-assisted creations. Central themes include authorship and inventorship, ownership of AI-generated outputs, use of copyrighted works in AI training datasets, transparency of data sources, and appropriate remuneration for rights holders. While the Conversation does not produce binding legal rules, it plays a critical normative role by clarifying areas of consensus and divergence, informing national law reforms, and guiding policy experimentation across jurisdictions. As a framework for AI governance, WIPO's approach emphasizes balance—aiming to safeguard human creativity and cultural production while fostering innovation—and supports a move away from strict compliance and toward flexible, values-driven governance that is cognizant of the particular difficulties AI presents for the creative and cultural sectors.

Regional and Domestic AI Regulatory Models

EU AI Act (risk-based approach and cultural exceptions): The EU Artificial Intelligence Act (AI Act) represents the most comprehensive binding legal framework for AI governance to date, shaping global regulatory approaches through its structured risk-based model (European Union, 2024). The Act classifies AI systems into unacceptable, high-risk, limited-risk, and minimal-risk categories, with regulatory obligations calibrated according to the level of potential harm to fundamental rights, safety, and societal interests. This approach is particularly significant for the creative and cultural industries, where many AI applications—such as generative content tools, recommendation systems, and cultural data analytics—fall outside strict prohibitions but raise substantial concerns regarding transparency, authorship, bias, and cultural representation. The AI Act introduces obligations on transparency, human oversight, and risk management for certain generative and general-purpose AI systems, including a requirement that AI-generated or manipulated content be marked as such, thereby embedding accountability beyond mere market compliance. Crucially, the

EU AI Act also reflects sensitivity to cultural and creative considerations through its interaction with EU constitutional values, fundamental rights, and sector-specific regimes such as copyright and media regulation. While the Act does not create explicit “cultural exceptions” in the traditional sense, its design allows space for the protection of freedom of expression, artistic freedom, and cultural diversity, notably through proportionality, exemptions for certain uses, and complementary application of IP and cultural policy instruments. By integrating AI regulation within the EU’s broader human-rights and cultural-policy framework, the AI Act shapes AI governance as a values-driven system that balances innovation with the preservation of human creativity, cultural pluralism, and democratic norms, making it a critical reference point for human-centered AI governance in the creative and cultural industries.

UK, US, and Global South perspectives: AI governance in the UK, US, and Global South reflects diverse regulatory philosophies that collectively shape the global legal landscape for artificial intelligence, particularly in the creative and cultural industries. The United Kingdom has adopted a principles-based, pro-innovation approach, relying on existing regulators and soft-law guidance rather than comprehensive AI legislation, with emphasis on safety, transparency, fairness, accountability, and contestability (United Kingdom Department for Science, Innovation and Technology, 2023). This flexible model allows creative industries to experiment with AI tools while raising concerns about regulatory fragmentation and uneven protection for creators’ rights. The United States, by contrast, maintains a largely market-driven and sector-specific framework, combining intellectual property law, competition law, and executive guidance—the trajectory of which shifted markedly when the 2023 federal executive order on trustworthy AI was revoked and replaced in early 2025 by a deregulatory, competitiveness-focused order—while courts increasingly shape AI governance through copyright and fair use litigation. This approach prioritizes innovation and free expression but often leaves gaps in protecting creative labour and cultural interests. In the Global South, AI governance is increasingly framed through the lens of development, digital sovereignty, and cultural preservation. Many states rely on international soft-law instruments, such as UNESCO and OECD

principles, while adapting them to local contexts marked by data dependency, infrastructure gaps, and the risk of cultural marginalization by dominant global platforms. For creative and cultural industries in these regions, AI governance is closely linked to concerns about data colonialism, equitable access, and the protection of indigenous knowledge and cultural expressions (Couldry & Mejias, 2019). Collectively, these perspectives illustrate that AI governance is not monolithic but context-sensitive, reinforcing the need for human-centered, values-driven frameworks that balance innovation with cultural diversity, creator protection, and inclusive development across jurisdictions.

Intellectual Property, Cultural Rights, and Labour Law Dimensions

AI governance in the creative and cultural industries is deeply intertwined with intellectual property (IP), cultural rights, and labour law, which together form a multidimensional legal framework shaping both the development and use of AI systems. IP law addresses questions of authorship, ownership, and protection of AI-generated works, ensuring that human creators retain recognition and economic rights, while also confronting challenges such as the use of copyrighted material in AI training datasets.

These questions are no longer abstract. In several jurisdictions, copyright protection turns on the presence of human authorship: in the United States, both the Copyright Office and the courts have confirmed that works generated autonomously by AI, without sufficient human creative contribution, are ineligible for registration (Thaler v. Perlmutter, 2025; United States Copyright Office, 2025). Other systems take a different path; the United Kingdom, for instance, retains a statutory provision attributing authorship of a “computer-generated work” to the person who makes the arrangements necessary for its creation, although the fit between that provision and modern generative systems is increasingly questioned (Copyright, Designs and Patents Act 1988, s 9(3)). A parallel and equally contested issue is the lawfulness of using protected works to train AI models. The European Union addresses this through text-and-data-mining exceptions that permit certain uses subject to a rights-holder opt-out, while

a growing body of litigation in multiple jurisdictions tests whether large-scale training on copyrighted material constitutes infringement or is excused as fair use or under a statutory exception (European Union, 2019). For the creative and cultural industries, the resolution of these questions will determine not only who owns AI-assisted outputs but also whether creators can meaningfully consent to, and be remunerated for, the use of their work as training data.

Cultural rights, rooted in international human rights law, emphasize the protection of cultural diversity, heritage, and community expression, highlighting the need to prevent cultural homogenization and marginalization that may result from AI-driven content generation. Labour law further contributes by safeguarding the rights and working conditions of creative professionals, protecting against exploitative practices, algorithmic management, and the displacement of human labour by automated systems. Together, these legal dimensions reinforce the importance of a human-centered, values-driven AI governance framework that not only ensures compliance with existing laws but also actively promotes creative autonomy, equitable remuneration, and the sustainable development of cultural ecosystems.

Key Governance Challenges In The Creative And Cultural Industries

The erosion of human creative agency has emerged as a critical governance challenge in the creative and cultural industries due to the growing integration of AI into creative processes. As generative algorithms increasingly participate in tasks such as content creation, composition, and design, the boundaries between human authorship and machine output become blurred, raising questions about who retains control, decision-making authority, and recognition for creative works. This erosion threatens not only the autonomy and originality of human creators but also the diversity and authenticity of cultural expression, as AI systems often replicate dominant styles, tropes, or commercially optimized patterns. Without appropriate governance measures, creators may become passive contributors, constrained by the logic and biases embedded in AI systems,

while platforms and developers wield disproportionate influence over cultural production.

Furthermore, bias, cultural homogenization, and data colonialism constitute a pressing governance challenge in the creative and cultural industries, arising from the ways AI systems are trained, deployed, and monetized. AI models rely on large datasets, which often disproportionately reflect dominant cultures, languages, and aesthetic norms, embedding systemic biases that marginalize minority creators and underrepresented cultural expressions. This can lead to cultural homogenization, where AI-generated outputs reinforce mainstream styles and trends at the expense of local, indigenous, or non-commercial forms of creativity, undermining cultural diversity and pluralism. The phenomenon of data colonialism exacerbates these issues, as global tech platforms often extract and exploit cultural data from the Global South without adequate consent, compensation, or recognition, concentrating power and economic benefits in the hands of a few multinational entities (Couldry & Mejias, 2019). Addressing this challenge requires governance frameworks that prioritize inclusive data practices, equitable access to AI technologies, and protection of cultural rights, ensuring that AI supports rather than diminishes the richness and diversity of human creative expression.

Lastly, power asymmetries between platforms and creators represent a significant governance challenge in the creative and cultural industries, driven by the concentration of technological, economic, and informational power in a few dominant AI-enabled platforms. These platforms often control access to audiences, data, and distribution channels, giving them disproportionate influence over what content succeeds commercially and culturally. Creators, by contrast, frequently operate under opaque algorithms, restrictive terms of service, and unequal bargaining positions, limiting their ability to negotiate fair remuneration, protect their intellectual property, or maintain creative autonomy. This imbalance can lead to exploitation, undervaluation of labour, and loss of control over cultural outputs, while reinforcing platform-centric content economies that prioritize engagement metrics over artistic quality or cultural significance.

These asymmetries are structural rather than incidental. Because platforms control the recommendation and discovery systems through which audiences encounter cultural goods, they exercise a form of gatekeeping power that determines visibility, and therefore income, while disclosing little about how their algorithms operate (Zuboff, 2019). Creators are frequently presented with non-negotiable, standard-form terms governing licensing, data use, and revenue sharing, and have limited recourse when those terms change. The integration of generative AI compounds the imbalance: the same platforms that distribute creators' work may also use it—often without specific consent or compensation—to train systems that generate competing content at marginal cost. The cumulative effect is a redistribution of value away from individual creators and culturally specific communities toward a small number of vertically integrated firms, with consequences for both the economic sustainability of creative labour and the long-term diversity of cultural production. Effective governance must therefore address not only individual transactions but the underlying concentration of infrastructural and informational power.

Taken together, these challenges—the erosion of creative agency, bias and data colonialism, and entrenched power asymmetries—share a common root: existing compliance-oriented frameworks neither anticipate nor adequately constrain the cultural and distributive harms of automated creativity. Diagnosing the problems, however, is only the first step. If governance is to move beyond compliance, it must rest on an affirmative set of normative commitments capable of guiding institutional design. The next section therefore sets out the principles that should underpin a human-centered AI governance framework for the sector.

Principles Of A Human-Centered Ai Governance Framework For The Creative And Cultural Industries

A human-centered AI governance framework for the creative and cultural industries must prioritize human agency and creative autonomy, ensuring that AI systems augment rather than replace human creators. This principle emphasizes meaningful human oversight at every stage of the creative

process, from ideation to production and distribution, while safeguarding the rights of authors to attribution, control, and decision-making over their works. By embedding agency into AI governance, creators retain the freedom to experiment, innovate, and assert their cultural and artistic identities, preserving the authenticity and diversity of creative expression.

Central to the framework is the promotion of fairness, inclusion, and cultural diversity, addressing biases inherent in AI training data and algorithmic decision-making. Governance mechanisms must ensure that underrepresented creators, minority cultures, and local artistic traditions are protected from marginalization and homogenization. This principle also advocates for equitable access to AI tools, participatory decision-making in AI deployment, and the establishment of mechanisms that recognize and fairly compensate contributions from diverse creators, reinforcing a just and inclusive creative ecosystem.

Transparency and accountability are foundational to human-centered AI governance, requiring AI systems to be explainable, auditable, and aligned with ethical standards. Creators, regulators, and audiences must be able to understand how AI influences content creation, curation, and distribution. Additionally, the framework emphasizes sustainability of creative labour and cultural ecosystems, ensuring that AI deployment does not undermine long-term economic, social, or cultural viability. Together, these principles create a governance model that balances technological innovation with human values, ethical responsibility, and the preservation of vibrant and resilient cultural industries.

Institutional And Stakeholder-Based Governance Model

Institutional and stakeholder-based governance models recognize that effective human-centered AI governance in the creative and cultural industries requires the coordinated participation of multiple actors across public, private, and civil society domains. Governments and regulators provide the legal and policy infrastructure, setting standards, enforcing rights, and facilitating capacity-building, while creative industry institutions such as guilds, collecting societies, and professional associations develop

codes of conduct, licensing schemes, and best practices tailored to sector-specific needs. AI developers and platforms bear responsibilities for ethical system design, transparency, and human-in-the-loop oversight, ensuring that algorithms support rather than undermine creative labour. The participation of creators and cultural communities in participatory governance systems ensures that AI deployment is informed by a diversity of voices, local knowledge, and cultural values. Institutional and stakeholder-based solutions bridge the gap between legal compliance and values-driven, human-centered regulation by integrating these actors within a cooperative, multi-layered governance ecosystem that promotes accountability, inclusivity, and resilience.

Designing An Integrated Human-Centered Ai Governance Framework

Designing an effective framework requires a multi-layered structure that integrates the various laws, regulations, and standards bearing on AI into a coherent whole. The framework proposed here comprises three interlocking layers. The first is a legal-foundation layer of binding rules that operate as a baseline deterrent on the most serious harms—for example, prohibitions on manipulative or rights-infringing systems, mandatory disclosure of AI-generated content, and enforceable rights of consent and remuneration for the use of creators' works as training data. The second is an institutional and technical layer, comprising the standards, codes of conduct, licensing schemes, auditing requirements, and human-in-the-loop design practices developed by regulators, collecting societies, guilds, and developers. The third is a participatory oversight layer, in which creators and cultural communities exercise a continuing supervisory role through consultation, representation, and redress mechanisms.

The value of this layered design is best illustrated by practice. The 2023 collective agreements negotiated by the Writers Guild of America and SAG-AFTRA offer a concrete model: they combine binding contractual rules (AI-generated material cannot displace a writer's credit), institutional machinery (joint committees that monitor technological change), and consent-based protections (informed consent and compensation for the use of a performer's

digital replica). Although sector-specific and jurisdictionally limited, these agreements demonstrate how human oversight, transparency, and remuneration can be operationalised rather than merely asserted. A general framework can translate such arrangements into a model provision—for example: “No AI system shall be used to generate, alter, or substitute a creative work derived from an identifiable creator’s output without that creator’s informed consent, attribution, and fair remuneration, and any AI-generated or AI-assisted output shall be disclosed as such.” Provisions of this kind give the framework’s principles determinate legal content.

Ethics and creativity must, in addition, be embedded into the framework by design. Because creativity is the very resource on which the cultural economy depends, governance must be calibrated so that it protects rather than stifles creative practice; design choices, defaults, and incentives should therefore be oriented toward sustaining and rewarding human creativity rather than displacing it.

Finally, the application of these principles must remain context-specific. The appropriate degree of regulatory intervention should be determined by reference to particular sectors, use-cases, and risks rather than by uniform generalisation, and the distinct legal, economic, and cultural circumstances of each jurisdiction must be taken into account. A regulatory approach proportionate for high-volume commercial music streaming may be ill-suited to a community heritage archive, and the framework must be flexible enough to accommodate that variation.

Policy Recommendations

In light of the foregoing analysis, the following six recommendations translate the proposed framework into specific and actionable measures for legislators, regulators, industry bodies, and platforms.

1. **Mandate Human Oversight and Participatory Decision-Making.** Regulators and industry bodies should require that AI systems used in the creative and cultural industries incorporate meaningful human oversight throughout the creative process. In concrete terms, this means establishing

a default rule that AI-generated material cannot be credited as the author of, or substitute for, a protected work; requiring that creators retain authorship and attribution rights in AI-assisted outputs; and mandating opt-in consent before a creator's works are used to train AI systems. These obligations can be implemented through both regulation and sector-wide collective agreements, building on existing models in which unions and producers have negotiated enforceable AI provisions.

2. **Implement Inclusive Data and Cultural Governance.** Governments, platforms, and AI developers should adopt policies that promote inclusive data practices and equitable access to AI technologies. This involves curating diverse, representative training datasets; maintaining auditable records of dataset provenance; compensating contributors fairly through collective licensing; and protecting local and indigenous cultural expressions from exploitation or homogenization. Embedding fairness and cultural sensitivity into data governance helps prevent the data-driven cultural marginalization associated with extractive practices.

3. **Establish Transparency, Provenance, and Disclosure Obligations.** Legislators should require clear labelling of AI-generated and AI-assisted content, machine-readable provenance metadata, and disclosure of the principal categories of works used to train generative systems. Such obligations—already foreshadowed by the transparency rules of the EU AI Act—enable creators to detect unauthorised use of their work, allow audiences to make informed choices, and provide the evidentiary basis for enforcing consent and remuneration rights (European Union, 2024).

4. **Reform Remuneration and Strengthen Collective Bargaining for Creative Labour.** Policymakers should ensure that creators share equitably in the value generated by AI systems trained on or deployed alongside their work. This can be achieved through statutory remuneration rights, collective licensing administered by collecting societies, and the express recognition of creators' and performers' rights to bargain collectively over AI use. Where individual creators lack bargaining power against dominant platforms,

collective mechanisms are essential to correcting the structural asymmetries identified above.

5. **Create Sector-Specific Regulatory Sandboxes and Cultural Impact Assessments.** Regulators should establish supervised regulatory sandboxes—as the EU AI Act now requires—allowing creative-sector AI tools to be tested under regulatory oversight before wide deployment. In parallel, providers of higher-risk cultural AI applications should be required to conduct a “cultural impact assessment,” modelled on the data-protection impact assessment, evaluating effects on creators’ rights, cultural diversity, and minority representation before deployment (European Union, 2024).

6. **Strengthen Protection of Indigenous Knowledge and Traditional Cultural Expressions.** Governments should align AI governance with emerging international instruments protecting traditional knowledge and traditional cultural expressions, ensuring that AI systems do not appropriate indigenous and community-held cultural material without free, prior, and informed consent and equitable benefit-sharing. This recommendation is particularly important for the Global South, where the risk of data colonialism and cultural extraction is most acute (World Intellectual Property Organization, 2024).

JIPPS
JOURNAL OF IP PROFESSIONALS

Conclusion

In conclusion, moving beyond mere compliance to a human-centered, values-driven AI governance framework is essential for safeguarding creativity, cultural diversity, and the rights of creators in the evolving landscape of the creative and cultural industries. By embedding principles of human agency, transparency, fairness, and accountability, and by engaging multiple stakeholders—including regulators, platforms, and cultural communities—AI can be harnessed to augment rather than replace human creativity. Such governance not only mitigates risks of bias, cultural homogenization, and labour exploitation but also ensures that AI contributes to sustainable, inclusive, and ethically responsible cultural innovation.

References

Attard-Frost, B., De los Ríos, A., & Walters, D. R. (2023). The ethics of AI business practices: A review of 47 AI ethics guidelines. *AI and Ethics*, 3(2), 389–406. <https://doi.org/10.1007/s43681-022-00156-6>

Hechler, E., Oberhofer, M., & Schaeck, T. (2020). AI and governance. In *Deploying AI in the enterprise* (pp. 165–211). Apress. https://doi.org/10.1007/978-1-4842-6206-1_8

Hesmondhalgh, D. (2018). *The cultural industries* (4th ed.). SAGE.

Copyright, Designs and Patents Act 1988, c. 48 (UK).

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

European Union. (2019). Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. *Official Journal of the European Union*, L130, 92.

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L2024/1689.

OECD. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449, amended 2024). Organisation for Economic Co-operation and Development.

Thaler v. Perlmutter, No. 23-5233 (D.C. Cir. Mar. 18, 2025), *aff'g* 687 F. Supp. 3d 140 (D.D.C. 2023), *cert. denied* (U.S. Mar. 2, 2026).

UNESCO. (2009). *The 2009 UNESCO framework for cultural statistics*. UNESCO Institute for Statistics.

UNESCO. (2021). Recommendation on the ethics of artificial intelligence (SHS/BIO/PI/2021/1). United Nations Educational, Scientific and Cultural Organization.

UNESCO. (2022). Culture and artificial intelligence: Impacts and policy considerations. United Nations Educational, Scientific and Cultural Organization.

United Kingdom Department for Science, Innovation and Technology. (2023). A pro-innovation approach to AI regulation (White Paper, CP 815). HMSO. (Government response published February 2024.)

United States Copyright Office. (2025). Copyright and artificial intelligence, Part 2: Copyrightability. Library of Congress.

World Intellectual Property Organization. (2019). Background document on intellectual property and artificial intelligence (WIPO/IP/AI/2/GE/20/1). WIPO.

World Intellectual Property Organization. (2024). WIPO Treaty on Intellectual Property, Genetic Resources and Associated Traditional Knowledge. WIPO.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

BRIDGING TRUST AND TRACEABILITY: REGULATORY COMPLIANCE CHALLENGES IN BLOCKCHAIN-ENABLED SUPPLY CHAIN FINANCE FOR AFRICAN EXPORTS

Yetunde Oluwafunbi Ajayi

Abstract

The 21st century has witnessed a sprout in the development of blockchain technology, which in turn indicates positive prospects in trade and supply chain financing. Blockchain has been praised for promoting transparency, real-time verifications, end-to-end traceability and immutability. However, uncertainty exists around its practical application to supply chain finance for the African Export market. Most especially because Africa continues to suffer from a trade deficit and is plagued by uncertain and heterogeneous regulatory regimes. This article examines the landscape in the African exports market from a legal and comparative perspective - with a view to identifying regulatory challenges, bottlenecks and opportunities for the practical application of Blockchain in Africa's supply chain financing. The article also identifies a few theories and notable practices, bridging the gap between the two worlds. The method employed by this work is the doctrinal, library based approach, which draws from regulations, treaties, industry publications and scholastic texts. This approach allows for the seamless synthesis and analysis of information from relevant sources. In all, the work concludes that; Blockchain births boundless opportunities for Africa to bolster its export supply chain however, regulation needs to be more proactive and purposive. This work then offers actionable recommendations to achieve the desired objectives.

Keywords: Blockchain, Trust, Traceability, Exports, Trade.

1. Background

There exists a deficit of funding and coordination in Supply Chain finance in the African Continent. Yet, translating the blockchain innovation into bankable finance and risk mitigation has its prospects and challenges (International Finance Corporation [IFC], 2025). For example, the disruption of the customs, traditions and existing status quo may lead to information asymmetry across markets - which blockchain ironically seeks to prevent.

This work takes the bold view that Blockchain-enabled supply chain financing will bridge trust and traceability for African exports. However, in reality, there exists regulatory and compliance challenges. Therefore, such an attempt will require coordinated political will and a unification of the heterogeneous legal and policy landscape governing finance, cybersecurity, anti-money laundering and counter-terrorist financing (AML/CFT) across independent and sovereign countries within the African continent (Reuters, 2024). For example, even though African countries recognize “electronic documents” their court systems still adopt traditional modes of contracting and proof in evidence (African Export-Import Bank [Afreximbank], 2024b).

To compound the problem, developers and early adopters may be faced with regulatory confusion and compliance frictions while attempting to deploy blockchain enabled smart contracts across jurisdictions. This work therefore provides an overview / review of:

- (i) data protection rules as it relates to cross-border situations (a few legislations like the Nigeria's Data Protection Act 2023 and the Kenyan Data Protection Act 2019 are discussed).
- (ii) financial-crime regulation, Anti-Money Laundering prohibitions (AML) and Know Your Customer (KYC) safeguards and guidelines (like the FATF standards).
- (iii) Gaps and loops in the continent's legal regime. Of particular concern here includes Africa's snail-paced adoption of the UNCITRAL Model Law on Electronic (Transferable) Records (MLETR) - amongst other treaties and

regulations. Laudable provisions of relevant laws from choice jurisdictions are also reviewed (like the UK's Electronic Trade Documents Act 2023) (Pelling, 2023).

(iv) The blockchain / security frameworks that will reduce regulatory conflicts and

(v) The sustainability of maintaining the status quo in a rapidly evolving world and how it affects the supply chain financing of African exporters. Here some notable sustainability regulations are also identified, like the EU-Deforestation Regulation (European Commission, 2025b).

This paper suggests “compliance-by-design” as a viable option to avoid possible regulatory conflicts. This means that the Blockchain solution should integrate parameters / architectures that can ensure (at least) a decent level of privacy while still ensuring traceability. This can be done by identifying transactions as a traceable and historical record of several transactions, rather than apportioning every single transaction to a person. Furthermore, this work suggests that an audit trail should be integrated in such architectures to enhance verification and cross-jurisdictional reference / governance (European Commission, 2024).

Given the peculiar background of Africa, this work suggests a phased policy implementation as this will facilitate long-term scale. At the onset, African governments should allow blockchain integration to be handled in collaboration with the private sector and should first govern by licensing before outright intervention. In practice, some nations implement the sandbox model where private entities are granted a limited license to try out their technology products without the requirement of a full license - the AfCFTA Digital Trade Protocol, and the Nigerian SEC Sandbox license and the CBN Sandbox licenses are credible examples of these (African Union, 2024a).

Finally, while actionable recommendations are made in this work, the regulators and governments will need to exercise purposive executive will, to advance the continent's supply chain financing to the desired future.

2. Theory and Literature Review

Trust has, over the years, become a recurring concern in international trade with Africa, both as it relates to micro and macro-economic phenomena. For example, allegations of non-performance or non-conformance to contractual terms may stem from intentional acts or innocent misrepresentations/promises. For example, the physical transportation of goods may be delayed, due to regulatory bottlenecks and bureaucratic processes that frequently affect international trade, while payment obligations may be frustrated by galloping inflation and foreign exchange risks. Trust, therefore, extends beyond the transacting parties themselves and is shaped by the broader systems, processes, terrains and logistic constraints within which trade occurs (Akinkugbe, 2025).

The Africa Export Import Bank has estimated the trade and SCF gap in Africa at US\$80–120 billion annually (Afreximbank, 2025). This figure is particularly troubling, given that SMEs make up the majority of businesses in Africa and its agricultural commodity value chains remain largely underdeveloped (International Trade & Forfaiting Association [ITFA], 2022). The situation is further compounded by high rejection rates arising from incomplete KYC documentation, compliance issues, and documentary risk. As a result, traceability has become a market-access necessity for supply chain financing in Africa (African Union, 2025). For example, in the European Union, national traceability systems have been rolled out to address concerns such as deforestation and other environmental risks (De Oliveira, 2024).

Global trade has experienced significant growth due to digitization (Bank for International Settlements [BIS], 2021). However, this acceleration remains uneven, with the African continent getting a smaller piece of the pie (OECD, 2025). While economists identify a “deficit” in the balance of trade as the common culprit, there are specific issues that lead to this result. As it relates to this topic, there is a dearth of supply chain finance as multi-national corporations and financial institutions disproportionately favour larger enterprises and publicly listed companies to the detriment of small and

medium-sized entities seeking to export at more competitive rates. The reason is not far-fetched. International players lack local knowledge of prospective applicants and will often prefer to proceed with a well-known entity. Financiers also find it inexpedient and expensive to trace small entities or enforce obligations in individual jurisdictions (African Union, 2024b).

Against this backdrop, blockchain presents an appealing and enticing solution which allows transparency, audit, real-time visibility and pre-programmable smart contracts. Ideally, these features would enable international players and financial institutions to manage multiple financing structures efficiently. In practice, however, this ideal often collides with reality as noted earlier (in the background above). Compounding these challenges is a high aversion to the judicial systems in African countries, which are widely seen to be slow, traditional and outdated.

3. Notable Considerations / Jurisdictions

The AfCFTA 2019: The African Free Continental Trade Area Agreement is a very ambitious project of the African Union, birthed from its Agenda 2063 - with the African Import Export Bank being the key driver of the goals towards “the Africa we want” (East African Community, 2022). Besides from being the World's largest free Trade Area Agreement (55 countries) it seeks to eliminate trade barriers, establish cross-country value chains and advance the development of value added trade. A prevalent challenge in African Trade is the paper based documentation and retrieval systems which make it difficult and time-consuming to trace, verify and establish transactions (First Fiduciary, 2025). The AfCFTA Digital Trade Protocol attempts to rectify the discrepancies in electronic evidentiary rules and provide a model law (which in turn) will reduce trade barriers and encourage intra-African trade (between African nations) and international trade (with African nations).

South Africa: Electronic documents are recognized under South Africa's Electronic Communications and Transactions Act. In *Spring Forest Trading 599-CC v Wilberry (Pty) Ltd* (2014), its Court upheld the validity of e-signatures. Under the Law of Evidence Act electronic documents are also admissible once the relevant foundation has been laid. From the case of *S v*

Ndiki (2007) and similar jurisdiction, once a foundation has been laid as to the relevance and validity of an electronic evidence, it will be recognized in court.

Nigeria: Section 84 of the Nigerian Evidence Act recognizes electronic / computer generated documents and provides that it can be admissible where the requisite foundation as to its validity has been laid. This provision has been confirmed in *Kubor v Dickson* (2012) and *Dickson v Sylva* (2016) and a host of other cases. Jurisprudentially, Nigerian courts are also admitting digital “records” as documents provided such data was generated from a machine that was properly working through the duration when such information was created (see Section 84(2) of the Evidence Act, *supra*).

Kenya: Similar to the position in Nigeria and South Africa, the Kenyan courts have recognised that electronic / computer generated documents are admissible in evidence, provided there was no alteration or tampering. See *Republic v Barisa Wayu Mataguda* (2011). Furthermore, in *Arunda v Office of the Data Protection Commissioner & Anr* (2025) the Court considered the constitutionality of Section 56 of the Data Protection Act 2019 and the constitutionality of Regulation 14 of the Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021 - upholding the right to privacy and data ownership. In the landmark *WorldCoin* case, *Republic v Tools for Humanity Corporation* (2025), the court mandated compliance with data protection laws particularly requiring the consent of the data subject and holding that the mode of collection (which in this case featured biometric and cryptocurrency issuance) has to fully comply with the provisions of the law. This decision should be instructive to blockchain developers while coding the fingerprinting and traceability algorithms.

United Kingdom: The English courts treat cryptoassets as property and adopt a fairly pragmatic approach towards electronic evidence. It is no longer news that electronic signatures and email correspondences are admissible in English courts until the contrary is proven. See *Golden Ocean Group Ltd v Salgaocar Mining Industries Ltd* (2012) and *Neocleous v Rees* (2019). Also, the UK Electronic Trade Documents Act 2023. Furthermore, in English

jurisprudence, there is a fiduciary requirement on developers / owners of such electronic records where it can be established that they have control. See *Tulip Trading Ltd v Van der Laan* (2023). From a jurisprudential standpoint, blockchain contracts can be proven. In *AA v Persons Unknown* (2019) the English Court recognized cryptocurrency as a form of property and was able to grant an injunction over misappropriated Bitcoin - holding that cryptocurrency is a form of property over which proprietary reliefs can be made (Yip, 2024). See also *Ion Science Ltd v Persons Unknown* (2020). One may ask how service of court processes will be effected in a situation between non-prives (for example spams and scam situations). In *D'Aloia v Persons Unknown & Ors* (2022), the Court allowed service by airdropping and utilized the doctrine of constructive trust in fraud. This is a forward-looking approach.

Singapore: Just like the United Kingdom, Singapore has been well reasoned in most of its laws and jurisprudential approach to digital assets. In *Quoine Pte Ltd v B2C2 Ltd* (2020) the Singaporean Court of Appeal directly examined the implication of trades done through algorithms on the blockchain. The Court validly construed liability on the exchange for breach of contract (although it hesitated to impose the doctrine of trust over the overall pooled assets of the exchange). In *CLM v CLN* (2022), the Court was able to grant freezing injunctions over stolen cryptocurrency noting that it was a property - while in *Janesh S/O Rajkumar v Unknown Persons* (2022), a similar injunction was granted over a non-fungible token. These decisions place Singapore as a noteworthy and forward-looking jurisdiction worthy of mention.

New Zealand: The New Zealand courts have drawn inspiration from the UK Courts on electronically admissible documents and applied the jurisprudential principles specifically to blockchain transactions. In *Ruscoe v Cryptopia (in liquidation)* (2020) the Court recognized cryptocurrency and applied the doctrine of trust to its assets. In contrast, many African jurisdictions are still catching up, lacking clear legal recognition of digital assets or guidance on handling blockchain-related disputes.

China: The Chinese courts have gained influence in recent times for their disciplined jurisprudence in this field. First, they have particularly recognized and do make strategic attempts to efficiently regulate blockchain through innovative legislations and technology / internet Courts. In 2018, blockchain evidence was accepted by the Hangzhou Internet Court in Hangzhou Huatai Media Culture Media Co., Ltd. v Shenzhen Daotong Technology Development Co., Ltd (2018), where it laid down salient principles for a Court's adoption of blockchain evidence, which (in summary) requires that:

- The Court considers the blockchain technology to see if it is tamper-proof and traceable.
- The electronic evidence or data stored should have a clear source and history.
- There has been no distortion or mutilation in transmission.
- Data can be verified from the platform or source code and (or) history/logs.

In this case, the data so analyzed complied with the requirements for reliability and was admitted in evidence.

4. Critical Analysis

From the above overview, it is clear that electronic evidence is admissible once the legal safeguards have been established. The regulators and Courts have applied property and equitable jurisprudence to bring blockchain within the ambit of the law to unlock the remedies under the law (injunctions, Mareva/freezing orders, tracing, amongst others). Electronic signatures and correspondences are also recognized in some African jurisdictions, hence smart contracts on the blockchain should implement sequences for signing and assent (whether through hashes, timestamps, audit trails or if-this-then-that codifications). With limited liability under the various privacy and data protection regulations, developers and contract drafters should ensure that the data subject is informed of the data being collected and does assent to

this. Given the foregoing, this work proposes “compliance by design” to avoid friction with regulators.

Compliance by Design: Key Parameters and Considerations

1. Data protection: Privacy and data protection are legal concerns that have become front burner issues in the digital age. In Nigeria, for example, the Data Protection Act 2023 creates the NDP Commission to regulate data processing and implement appropriate safeguards on the collection and use of data (CMS Law, 2022). Likewise, in Kenya, its Data Protection Act 2019 codifies similar protections. South Africa's data protection law additionally requires that in international transfers, the recipient jurisdiction should be data compliant. Similar provisions of other African countries can be seen to be similar to the GDPR (Information Technology & Innovation Foundation [ITIF], 2025). AML/CFT: FATF (R-15) seeks to entrench some level of AML best practices and compliance for Virtual Asset Service Providers (Financial Action Task Force [FATF], 2024a) and requires (at the very least) the originator/beneficiary information (FATF, 2024b). Much remains to be felt on its implementation, which is uneven across jurisdictions and platforms.

A split ledger pattern can be adopted to balance the competing rights to privacy with the need for transparency. This means that personal/private information will be off chain while transactional data, hashes and metadata will be on chain. Access to this information can also be integrated through REST Application Programming Interfaces (APIs) so that it shows as a record and further details can be received, either by a consent to the transfer, or by additional regulatory intervention.

2. Regulatory Synchronisation: Regulators tend to retrospectively regulate the fintech sectors through ambiguous bans and restrictions. For example, in 2021, the Central Bank of Nigeria prohibited banks from facilitating crypto transactions. However, subsequent regulations have been issued in collaboration with the Securities and Exchange Commission (in 2023 and 2024) to ease the tightening by introducing a Sandbox regime and an AIRP licence (Approval in Principle). In 2024, the Bank of Ghana also proposed draft guidelines which (in sum) recommended a risk-based approach to

regulating fintechs and digital assets (and offered a sandbox solution) (Bank of Ghana, 2024).

3. Documentary Evidence and Enforceability: The UNCITRAL Model Law on Electronic Transferable Records (2017) admonishes / canvasses for the admissibility of electronic documents. What this means is that countries may agree that the paper equivalents of trade documents like bill of lading and promissory notes can be translated to digital representations having evidential value in the jurisdiction that chooses to adopt its provisions. Developed countries like Singapore, UK and France, have made purposive adoptions to their local regulations (for example, the UK's Electronic Trade Documents Act 2023), however, the adoption in Africa remains limited and uneven (United Nations Commission on International Trade Law [UNCITRAL], 2017). Parties transacting with Africa may utilize smart drafting to select the United Kingdom as the choice of law and jurisdiction - however, these approaches do not totally preclude a local party from suing in its local courts unless a detailed dispute resolution clause is provided in the contract. International companies may therefore opt to deal with entities in UNCITRAL-compliant jurisdictions to avoid complications in collateral enforcement. This does not mean that Africa is without rescue (World Customs Organization [WCO], 2025). For example, South Africa, in its Electronic Communications and Transactions Act, grants legal backing to electronic signatures while Nigeria, in Section 84 of its Evidence Act (2011), provides for the admissibility of electronic / computer-generated evidence (subject to the provision of a certificate of authentication if it is sought to be tendered in litigation). It is arguable that blockchain records can be classified as computer-generated / electronic documents under these provisions.

4. Sustainability: A compliant-by-design blockchain implementation will have to integrate standards and metrics that ensure long-term sustainability of both the systems and the entities it impacts. For example, traceability systems should be put in place for the trade in environmentally sensitive crops (like cocoa) including ID mapping, geolocation proofs and zero-knowledge proofs (European Forest Institute, 2025).

5. Conclusion and Recommendations

Transparency and traceability can be improved by the integration of blockchain to Africa's Supply Chain Financing. However, this can only be achieved by reducing compliance friction across jurisdictions. This therefore validates the case for blockchain compliance by design - where issues of permitted-privacy, sustainability proofs, AML/CFT compliance and constitutional benchmarks are implemented. The possibilities are endless; faster access to capital, bolstered trade and innovation in our supply value chain are just a few. This work proceeds to provide the following actionable recommendations, drawn together from the discussion above:

A. Convert Model laws to model blockchains, hashes, audit logs and risk utilities for independent implementation by interested governments, entities, institutions and parties. Preference should be placed on interoperability and specific performance.

B. Adopt standard contractual clauses and map legal data across the continent (this will require cooperation among states / the adoption of UNREFERENCED REFERENCE REFERENCED ITRAL models).

C. Choose a mature jurisdiction: contracting parties can nominate more advanced jurisdictions like China and the United Kingdom as the forum for litigation and the choice of law.

D. African nations should align with the provisions of the AfCFTA (African Development Bank [AfDB], 2024) (this will require strong political will).

E. Encourage inter-governmental and cross-country API integrations to encourage (limited but) shared registries and avoid duplication.

F. Democratise the sandbox initiative for Virtual Asset Service Providers.

G. Implement audit trails that can serve as verifiable records so that they fall within the ambit of electronic correspondence under the lines of Nigerian and South African law.

H. To guard against cyberattacks and fraud, clients' funds should be segregated from the live server or held in trust - in line with the decisions examined earlier.

Africa features countries with their various laws. Under the constitutional law of certain African countries (like the Federal Republic of Nigeria), the country's adoption of an international treaty does not automatically translate to local enforcement or application. There is an additional requirement for such laws to be “domesticated” through a re-enactment in the local legislation of that country. This will therefore require sufficient pressure from international organizations (first) by making the domestication of reputable model laws a pre-condition for the grant of loans or financial aid.

References

African Development Bank. (2024). 2024 annual report. <https://www.afdb.org/en/documents/annual-report>

African Export-Import Bank. (2024b). Afreximbank annual report 2023. <https://www.afreximbank.com/annual-report-2023>

African Export-Import Bank. (2025). African trade report 2025: African trade in a changing global financial architecture.

African Union. (2024a). Protocol to the agreement establishing the African Continental Free Trade Area on Digital Trade. <https://au.int/en/treaties/protocol-agreement-establishing-african-continental-free-trade-area-digital-trade>

African Union. (2024b). Africa seeks a new financial landscape to address debt, risk ratings and cost of capital (Press Release No. 000003456/2024/17/02).

African Union. (2025, February 7). African leaders convene on establishment of homegrown solution: The Africa Credit Rating Agency (AfCRA) [Press release].

Akinkugbe, O. (2025). Strengthening the African financial architecture: Why African multilateral financial institutions should have the same preferred creditor status as MDBs' analysis. Afronomics Law. <https://www.afronomicslaw.org/category/analysis/multi-national>

Bank for International Settlements. (2021). Central bank digital currencies: Foundational principles and core features (Public consultation paper). <https://www.bis.org/publ/othp68.pdf>

Bank of Ghana. (2024, August). Draft guidelines on digital assets. <https://www.bog.gov.gh/wp-content/uploads/2024/08/Draft-Guidelines-on-Digital-Assets.pdf>

CMS Law. (2022). Managing cross-border data transfers (CMS/ZAF/7/2022).

De Oliveira. (2024). The European Union and United Kingdom's deforestation regulations: Implications for supply chain traceability and environmental governance. Environmental Science & Policy.

East African Community. (2022). African Continental Free Trade Area (AfCFTA) agreement. <https://www.eac.int/trade/international-trade/trade-agreements/african-continental-free-trade-area-afcfta-agreement>

European Commission. (2024, July 25). Corporate sustainability due diligence. <https://commission.europa.eu/business-economy-euro/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence>

European Commission. (2025b, October 21). Carbon Border Adjustment Mechanism (CBAM). <https://taxation-customs.ec.europa.eu/carbon-border-adjustment-mechanism>

European Forest Institute. (2025). Workshop: How Ghana and the EU are preparing for the EUDR. <https://efi.int/news/workshop-highlights-how-ghana-and-eu-are-preparing-eudr-2025-06-27>

Financial Action Task Force. (2024a). Status of implementation of Recommendation 15 by FATF members and jurisdictions with materially important VASP activity. <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf>

Financial Action Task Force. (2024b). Targeted update on implementation of the FATF standards on virtual assets/VASPs. <https://www.fatf-gafi.org>

First Fiduciary. (2025). AfCFTA and blockchain: Boosting transparency of trade. https://firstfiduciary.ng/wp-content/uploads/2025/01/AfCFTA-and-Blockchain-_Boosting-Transparency-of-Trade.pdf

Information Technology & Innovation Foundation. (2025, June 2). South Africa's cross-border data transfer regulation. Big Tech Policy Tracker.

International Finance Corporation. (2025). Scaling up supply chain finance could unlock billions for SMEs. <https://www.ifc.org/en/interviews/2025/>

International Trade & Forfeiting Association. (2022). Sustainable trade finance and African trade. https://itfa.org/wp-content/uploads/2022/10/ITFA_Sustainable-Trade-Finance-and-African-Trade

OECD. (2025). Trade facilitation indicators: Monitoring policies up to 2025. OECD Publishing. <https://doi.org/10.1787/fd6f27dc-en>

Pelling, S. (2023, June 28). Issues in cryptocurrency fraud claims—An update [Conference presentation]. 4th Annual Crypto in Disputes Conference, Judiciary.uk Thought Leaders.

Reuters. (2024, May 7). Nigeria plans additional rules to combat illegal trading in digital assets. <https://www.reuters.com/technology/nigeria-plans-additional-rules-combat-illegal-trading-digital-assets-2024-05-07/>

United Nations Commission on International Trade Law. (2017). UNCITRAL model law on electronic transferable records.

https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status

World Customs Organization. (2025). Responding to emerging challenges and paving the way for a secure future.

Yip, M. (2024). Mareva injunction and crypto fraud. In *Fraud and risk in commercial law* (pp. 123–143). https://ink.library.smu.edu.sg/sol_research/4487

Table of Cases

AA v Persons Unknown [2019] EWHC 2556 (Comm).

Arunda v Office of the Data Protection Commissioner & Another, CP (KLR) [2025] 12262.

CLM v CLN [2022] SGHC 46.

D'Aloia v Persons Unknown & Ors [2022] EWHC 1723 (Ch).

Dickson v Sylva (2016) LPELR-41257 (SC).

Golden Ocean Group Ltd v Salgaocar Mining Industries Ltd [2012] EWCA Civ 265.

Hangzhou Huatai Media Culture Media Co., Ltd. v Shenzhen Daotong Technology Development Co., Ltd (2018) Zhe 0192 Civ. HICC, No. 81.

Ion Science Ltd v Persons Unknown (Unreported, 21 December 2020).

Janesh s/o Rajkumar v Unknown Person (Board Ape NFT) (CHEFPIERRE) [2022] SGHC 264.

Kubor & Anor v Dickson (2012) CLR 10(c) (SC).

Neocleous v Rees [2019] EWHC 2462 (Ch).

Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.

Republic v Barisa Wayu Mataguda [2011] 1481 (KLR).

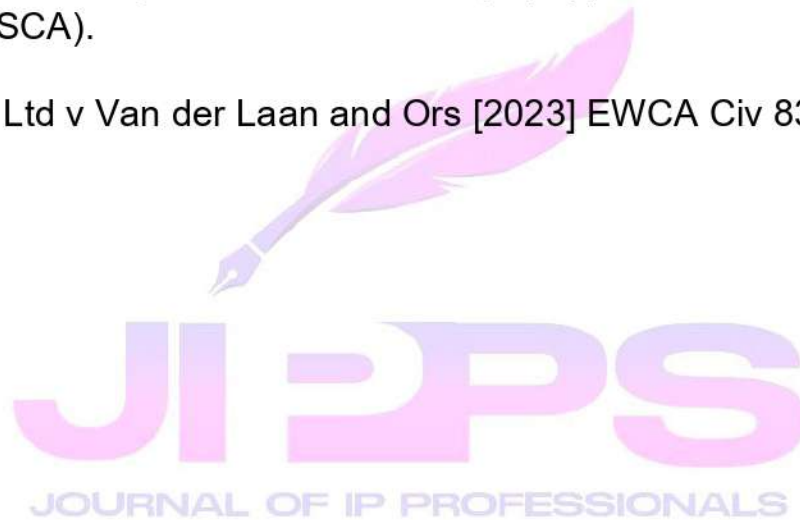
Republic v Tools for Humanity Corporation (US) & 8 Others; Katiba Institute & 4 Others (Ex parte Applicants) (JR-E119 of 2023) [2025] 5629 (KLR).

Ruscoe v Cryptopia Ltd (in liquidation) [2020] NZHC 728.

S v Ndiki and Others [2007] 2 All SA 185 (Ck).

Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash [2014] ZASCA 178 (SCA).

Tulip Trading Ltd v Van der Laan and Ors [2023] EWCA Civ 83.



AFRICA'S CROSS-BORDER DATA FLOW GOVERNANCE DEFICIT AND THE PATH TO A COHERENT LEGAL FRAMEWORK

Sinmiloluwa Adesanya

Abstract

Africa stands at a defining juncture in the governance of cross-border data flows. On one side, a wave of national data protection legislation, informed by the European General Data Protection Regulation (GDPR) and driven by aspirations of digital sovereignty, is producing localisation requirements and adequacy conditions that fragment the continent's data ecosystem. On the other hand, the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol, adopted in February 2024 with its eight annexes approved in February 2025, promotes the free flow of data across borders as a prerequisite for a functioning African single digital market. These two frameworks are not inherently irreconcilable, but the absence of a coherent, Africa-centred governance architecture to mediate between them, particularly how the Malabo Convention and AfCFTA DTP complement or conflict, creates a structural deficit, one that disadvantages African data subjects, African businesses, and African states alike. This article examines the nature of that deficit, the competing frameworks that produced it, and the conditions necessary for a workable resolution. It argues that Africa does not need to choose between sovereignty and integration; it needs a governance framework grounded in its own continental legal instruments, principally the Malabo Convention and the AfCFTA Digital Trade Protocol, that enables protected data flows rather than paralysing them.

Keywords: cross-border data flows, data governance, AfCFTA Digital Trade Protocol, Malabo Convention, data localisation, data sovereignty, African digital economy, regulatory fragmentation, personal data protection, IP and data

Introduction

Data is the operative currency of the digital economy. Its movement across borders enables cloud computing, digital financial services, e-commerce, artificial intelligence training, and the global commercialisation of intellectual property (Raji, R. 2022). For Africa, a continent of 55 states with a combined population projected to reach 2.5 billion by 2050, the governance of cross-border data flows is not only a secondary policy concern, but also a question about who controls the infrastructure of the digital economy, who benefits from it, and on whose terms, it operates (Future of Privacy Forum, 2025).

In the past five years, there has been an acceleration of legislative activity on the African continent. As of the end of 2024, 39 of Africa's 55 countries had enacted data protection laws, and 34 had established formal data protection authorities (DPAs) (Africa Privacy Roundup, 2024; Tech Hive Advisory, 2025). In 2024 alone, countries such as Cameroon, Ethiopia, and Malawi, enacted new frameworks (Africa Privacy Roundup, 2024). While all three laws include provisions for cross-data transfers, their depth varies. For example, Cameroon's law includes conditions for cross-border transfers and states that any international transfer of personal data requires prior authorisation from the DPA (Tech Hive Advisory, 2025). On the other hand, Malawi bars outbound transfers unless the destination country meets an adequacy standard or the parties have put in place recognised safeguards such as binding corporate rules (ITLawCo, 2024).

For countries with already established frameworks, such as South Africa's Protection of Personal Information Act (POPIA), the Act restricts cross-border transfers to jurisdictions that offer adequate protection similar to Malawi (Republic of South Africa, 2013). Nigeria is moving in a similar direction, with a localisation proposal for defined data categories currently under active consideration (Republic of Nigeria, 2023; Tech Hive Advisory, 2025). Ghana's 2025 draft Data Protection Act would require domestic storage of sensitive personal information, including biometric, health, and children's data (Republic of Ghana, 2025).

At the continental level, the trajectory appears to point in the opposite direction. In February 2024, the AfCFTA Digital Trade Protocol (DTP) was adopted at the 37th African Union Summit in Addis Ababa, accompanied by eight annexes that were approved in February 2025 (African Union Assembly, 2024, 2025). The Protocol establishes a framework premised on the free flow of data as a condition for digital trade among member states and prohibits data localisation requirements except in narrowly defined circumstances of legitimate public policy or national security necessity (African Union Assembly, 2024; Covington & Burling LLP, 2024).

The result of the multilayered provision for cross-border transfers is a governance architecture that is simultaneously over-legislated and under-coordinated. Individual states enact increasingly stringent data protection regimes while committing, at least notionally, to a continental protocol that constrains those same regimes. Businesses operating across African borders face a compliance environment in which the rules applicable to a single data transfer may differ materially depending on whether the originating state has enacted data protection legislation, whether it has established a functioning DPA, whether the destination state is deemed adequate under the originating state's law, and whether continental commitments apply (Future of Privacy Forum, 2025; Interoperability, 2025). This is not a sustainable basis for a functioning African digital single market.

This article proceeds in three parts. The first examines the two competing forces, national data sovereignty and continental integration, and the legal instruments through which they are expressed. The second analyses the governance deficit that their tension produces, drawing on specific country examples and the structural limitations of current frameworks. The third advocates for a coherent, Africa-centred path forward—one that leverages existing continental instruments like the Malabo Convention and AfCFTA DTP—to harmonise national policies with continental objectives, thereby reducing compliance complexity and fostering a unified digital economy.

2. Discussion

2.1 The Sovereignty Perspective: National Data Protection and the Localisation Trend

The expansion of data protection legislation across Africa reflects a legitimate policy concern. To contextualise the issue, Statista reports show that Africa has the world's youngest population and is among the fastest-growing adopters of digital technology (Statista, 2024a, 2024b). This combination is generating personal data at a scale and pace that few other regions can match. African citizens produce vast quantities of data through mobile payments, health applications, social media, and e-commerce every day, and that volume will only increase as connectivity deepens (Statista, 2024b). The overwhelming majority of this data is processed and stored on infrastructure located outside the continent (Raji R, 2022). Data localisation and adequacy requirements represent an attempt to redress this asymmetry: to ensure that African states retain meaningful regulatory jurisdiction over data generated by their citizens, and that those citizens can exercise the legal rights to which data protection law entitles them.

The Malabo Convention, formally, the African Union Convention on Cyber Security and Personal Data Protection, entered into force in June 2023] after achieving the required number of ratifications (African Union, 2023). While its provisions establish a continental baseline for data protection grounded in fundamental rights principles, policymakers may question its enforceability across diverse legal systems and the mechanisms for ensuring compliance. Its influence is growing, even among states that have not yet ratified it, but clarity on how it will be implemented and monitored remains essential for effective governance.

Yet the manner in which individual states are implementing data sovereignty objectives varies widely, and the divergence is itself a governance problem. South Africa's POPIA imposes an adequacy standard for outbound transfers but does not provide the clarity businesses need to assess what constitutes adequate protection in practice (Information Technology and Innovation Foundation, 2026; Republic of South Africa, 2013). Kenya initiated

discussions with the European Commission in 2024 to seek an adequacy determination, a milestone that, if achieved, would ease data flows between Kenya and the EU but would do nothing to address intra-African data movement (European External Action Service, 2024). In 2024, Rwanda published Standard Contractual Clauses to facilitate transfers; Uganda has also announced plans to revise its framework to allow more flexible transfer mechanisms (Africa Privacy Roundup, 2024). Morocco, Ghana, and Nigeria each apply different standards and different institutional architectures (Tech Hive Advisory, 2025).

The consequence is that intra-African data flows, precisely the flows that the AfCFTA digital single market depends on, are subject to a patchwork of divergent national rules with no common mechanism for mutual recognition (Future of Privacy Forum, 2025). Hence, a business operating across five African jurisdictions cannot rely on any single compliance framework.

2.2. The Integration Imperative: The AfCFTA Digital Trade Protocol and Its Tensions

The AfCFTA Digital Trade Protocol represents the most significant multilateral digital governance instrument Africa has produced (African Union Assembly, 2024). The protocol's provisions on cross-border data flows, particularly Article 20, which requires member states to permit the free flow of data subject to narrowly defined exceptions, are modelled on frameworks developed in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and comparable instruments (Comprehensive and Progressive Agreement for Trans-Pacific Partnership, 2018; Sucker, 2025).

The modelling choice for the Protocol has attracted pointed criticism. Scholars including Gathii (2024) and Beyleveld and Sucker (2023), have noted that the cross-border data flow provisions, as drafted, would grant substantial rights to any company incorporated in an AfCFTA member state, including subsidiaries of large foreign technology companies, to transfer African citizens' personal data to any jurisdiction, subject only to the company's own data protection practices. Under such a framework, a foreign

technology company incorporated in Kenya could transfer data collected from users across the continent to servers in the United States or China, with limited recourse for the individuals whose data is involved (Gathii, J. T, 2024; Beyleveld & Sucker, 2023).

A further tension concerns intellectual property. The AfCFTA DTP's provision on source code, Article 25, would prohibit member states from requiring access to software source code as a condition of market entry (African Union Assembly, 2024). Critics argue this goes beyond existing global intellectual property protections by effectively granting software firms greater secrecy rights than any IP regime currently provides, and limits governments' ability to scrutinise the algorithms that determine how African citizens' data is processed (Gathii, J. T, 2024). Proponents counter that the provision is necessary to prevent disguised trade protectionism and that technology transfer occurs more effectively in IP-protected environments, as evidenced by the significant growth in cross-border patent flows from developed to developing countries observed over recent decades (International Institute for Sustainable Development, 2024; Stuart, 2024).

The protocol's ratification process adds a further layer of complexity. Entry into force requires approval by 22 of the 55 AU member states, after which ratifying states will have an additional five years to align their national legislation (African Union Assembly, 2024; Covington & Burling LLP, 2024). The AfCFTA currently covers 49 of 55 AU member states as of 2025 (tralac Trade Law Centre, 2025). This means that for a substantial transitional period, potentially a decade or more, the continent will operate under simultaneously applicable national frameworks, the Malabo Convention baseline, and the AfCFTA DTP, without any settled hierarchy of norms or effective mechanism for resolving conflicts between them (Rutenberg & Ncube, 2025).

2.3. The Governance Deficit: What the Current Architecture Cannot Do

The governance deficit that emerges from this landscape has three structural dimensions.

First, there is no effective mechanism to facilitate intra-African data flows. The tools that exist elsewhere, adequacy decisions, mutual recognition agreements, binding corporate rules, and standard contractual clauses, are available in some African jurisdictions but have not been developed into any continental equivalents (Future of Privacy Forum, 2025). Kenya can seek an adequacy decision from the European Commission (European External Action Service, 2024). Still, there is no comparable mechanism by which Kenya can recognise South Africa's POPIA as providing adequate protection for data flowing from Kenya to South Africa, or vice versa. The Malabo Convention provides a normative baseline but no operational transfer mechanism (African Union, 2023). The AfCFTA DTP provides a free-flow commitment but leaves the conditions for exceptions, and the specific public policy objectives that justify them, to be elaborated by the Annex on Cross-Border Data Transfers, which, while adopted in February 2025, has not yet entered into force (African Union Assembly, 2025; tralac Trade Law Centre, 2025).

JOURNAL OF IP PROFESSIONALS

Second, the enforcement architecture is fragmented and under-resourced. Even where data protection laws exist, and DPAs have been established, enforcement capacity varies enormously. Many African DPAs lack the staff, technical expertise, and financial resources necessary to conduct investigations, process complaints, or engage meaningfully in cross-border cooperation (CIPEA, 2025; Digital Policy Alert, 2025). Criminal convictions for data protection offences, a recent development in Uganda and South Africa, signal a hardening enforcement posture, but individual enforcement actions cannot substitute for systemic regulatory coordination (Digital Policy Alert, 2025). The absence of a continental enforcement cooperation mechanism makes cross-border data protection violations involving multiple African jurisdictions very difficult to address.

Third, the interests of African data subjects, individuals whose data is at the centre of this governance debate, are structurally subordinated in both the sovereignty and integration frameworks. National data sovereignty rhetoric often prioritises state control over data flows rather than individual rights. The AfCFTA DTP's free-flow provisions prioritise the interests of digital trade and, as some critics argue, the companies that conduct it (Gathii, J. T, 2024, Mwangi et al., 2025). Neither framework, as currently constituted, provides African citizens with meaningful, practically enforceable rights over their personal data in the context of cross-border transfers. The Malabo Convention's rights-based framing provides the most coherent starting point, but its limited ratification undermines its practical force (African Union, 2023).

3. Conclusion: Toward A Coherent Africa-Centred Framework

The diagnosis presented above, competing national and continental frameworks, no effective transfer facilitation mechanism, under-resourced enforcement, and structurally marginalised individual rights, does not support a counsel of despair. Africa has the legal instruments necessary for a coherent framework. What it lacks is the institutional architecture and political will to operationalise them.

A workable path forward requires three connected elements. The first is a continental mutual recognition framework built on the Malabo Convention baseline. States that have enacted data protection legislation meeting the Malabo Convention's minimum standards should be able to recognise each other's frameworks as providing adequate protection for intra-African transfers, without requiring bilateral adequacy negotiations or resort to contractual mechanisms (African Union, 2023; Future of Privacy Forum, 2025). The AfCFTA Secretariat and the African Union Commission are the appropriate institutional actors to develop the assessment criteria, and the Annex on Cross-Border Data Transfers provides the legal hook on which such a framework can be anchored (African Union Assembly, 2025).

The second element is a differentiated approach to data localisation and free-flow commitments. The AfCFTA DTP's current framing, free flows as the default, exceptions narrowly available, may be appropriate for commercial

personal data in non-sensitive sectors (African Union Assembly, 2024). It is not appropriate for categories of data that carry heightened risk: biometric data, health records, children's data, financial records, and data critical to national security. African states need, and the protocol should accommodate, a tiered governance model that applies different rules to different categories of data, with the categories defined at the continental level to prevent fragmentation. This is consistent with the approach taken in existing African data protection laws, which almost uniformly distinguish between sensitive and non-sensitive personal data (Tech Hive Advisory, 2025).

The third element is a continental enforcement cooperation mechanism, a standing forum through which African DPAs can conduct joint investigations, share regulatory intelligence, and coordinate responses to cross-border violations. The Global Privacy Assembly, the International Conference of Data Protection and Privacy Commissioners, and the network of European data protection authorities under the GDPR's consistency mechanism all offer partial models. Africa needs its own version, housed within the African Union institutional framework, adequately resourced, and empowered to issue binding recommendations to national DPAs in cases involving cross-border harm.

None of this requires Africa to choose between sovereignty and integration. The dichotomy is false. Sovereignty, properly understood, is not the power to prohibit data from crossing borders; it is the capacity to set the terms on which data crosses borders and to enforce those terms. Integration, properly understood, is not the abolition of regulatory difference; it is the creation of a common legal space within which regulatory differences are managed rather than compounded. A coherent African data governance framework can honour both.

The digital economy will not wait for this framework to mature at its own pace. The AfCFTA DTP's ratification process, the continued expansion of national data protection legislation, and the accelerating deployment of artificial intelligence systems that process African citizens' data at scale all

create urgency (Rutenberg & Ncube, 2025). Africa has built the normative foundations. The task now is to build the governance architecture that makes them work.

References

African Union. (2023). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union Commission.

African Union Assembly. (2024, February). Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade (AfCFTA Digital Trade Protocol). 37th Ordinary Session, Addis Ababa, Ethiopia.

African Union Assembly. (2025, February). Annexes to the AfCFTA Protocol on Digital Trade. 38th Ordinary Session.

Africa Privacy Roundup. (2024). Roundup on data protection in Africa 2024. <https://africaprivacyroundup.com/roundup-on-data-protection-in-africa-2024/>

Beylevel, A., & Sucker, F. (2023). Regulating cross-border data flows under the AfCFTA Protocol on Digital Trade: The what, why, how, where, and when [Working Paper]. SSRN. <https://ssrn.com/abstract=4437331>

CIPESA. (2025). State of internet freedom in Africa report. <https://cipesa.org/2025/09/state-of-internet-freedom-in-africa-report/>

Comprehensive and Progressive Agreement for Trans-Pacific Partnership. (2018, December 30). Comprehensive and Progressive Agreement for Trans-Pacific Partnership. <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/cptpp/>

Covington & Burling LLP. (2024, February). Africa technology regulatory update: Adoption of the AfCFTA Protocol on Digital Trade. <https://www.cov.com/en/news-and-insights/insights/2024/02/africa->

technology-regulatory-update-adoption-of-the-afcfta-protocol-on-digital-trade

Digital Policy Alert. (2025). The year of the teeth: Data protection in Africa roundup 2025, projections for 2026. <https://digitalpolicyalert.org/blog/data-protection-in-africa-roundup>

European External Action Service. (2024, May 7). Data protection: Kenya and the EU launch the very first adequacy dialogue on the African continent. European Union Delegation to Kenya. https://www.eeas.europa.eu/delegations/kenya/data-protection-kenya-and-eu-launch-very-first-adequacy-dialogue-african-continent_en?s=352

Future of Privacy Forum. (2025). Cross-border data flows in Africa: Examining policy approaches and pathways to regulatory interoperability [Issue Brief]. <https://fpf.org/blog/cross-border-data-flows-in-africa-examining-policy-approaches-and-pathways-to-regulatory-interoperability/>

Gathii, J. T. (2024, February 20). The AfCFTA's digital trade rules are not fit for Africa. Afronomicslaw. <https://www.afronomicslaw.org/category/analysis/afcftas-digital-trade-rules-are-not-fit-africa>

IAPP. (2025). Evaluating data privacy across Africa: Toward a unified GDPR-inspired framework. <https://iapp.org/news/a/evaluating-data-privacy-across-africa-toward-a-unified-gdpr-inspired-framework>

International Institute for Sustainable Development. (2024). The AfCFTA Digital Protocol [Policy Analysis]. <https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol>

Information Technology and Innovation Foundation. (2026, February). South Africa's cross-border data transfer regulation. <https://itif.org/publications/2025/06/02/south-africa-cross-border-data-transfer-regulation/>

ITLawCo. (2024). Malawi's Data Protection Act 2024: An overview. <https://itlawco.com/focus-areas/malawis-data-protection-act-2024-an-overview/>

Mwangi, K., Adewale, A., & Senghor, J. (2025, December). Evolving approaches to cross-border data flows: Latin American and African perspectives. *International Data Privacy Law*. <https://doi.org/10.1093/idpl/ipaf037>

Raji, R. (2022, September 15). Where is Africa in the cloud? NTU-SBF Centre for African Studies, Nanyang Technological University. <https://www.ntu.edu.sg/cas/news-events/news/detail/where-is-africa-in-the-cloud>

Republic of Ghana. (2025). Draft Data Protection Act, 2025 [Consultation draft].

Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. Official Gazette.

Republic of South Africa. (2013). Protection of Personal Information Act, No. 4 of 2013 (POPIA). Government Gazette.

Republic of South Africa. (2024). National Policy on Data and Cloud 2024. Government Gazette No. 50741.

Rutenberg, I., & Ncube, C. (2025). Alignment problems: The AfCFTA Digital Trade Protocol and AI. *Research ICT Africa / Just AI*. https://researchictafrica.net/wp-content/uploads/2025/02/Alignment-problems-AfCFTA-digital-trade-protocol-AI_Just_AI_2025.pdf

Statista. (2024a). African countries with the lowest median age as of 2023. <https://www.statista.com/statistics/1121264/median-age-in-africa-by-county/>

Statista. (2024b). Number of internet users in Africa as of October 2024, by country. <https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/>

Stuart, J. (2024). The AfCFTA Digital Trade Protocol: Clarification of key issues. tralac Trade Law Centre. <https://www.tralac.org/blog/article/16325-the-afcfta-digital-trade-protocol-clarification-of-key-issues.html>

Sucker, F. (2025). The AfCFTA Digital Trade Protocol [Working Paper]. SSRN. <https://ssrn.com/abstract=5386851>

Tech Hive Advisory. (2025). Roundup on data protection in Africa 2024: Projections for 2025. <https://www.techhiveadvisory.africa/insights/roundup-on-data-protection-in-africa-2024-projections-for-2025>

tralac Trade Law Centre. (2025). Summary of the annexes to the AfCFTA Protocol on Digital Trade. <https://www.tralac.org/documents/events/tralac/5918-2025-conference-two-pager-summary-of-the-annexes-to-the-afcfta-protocol-on-digital-trade/file.html>



TECHNOLOGY AND SPACE LAW: WHERE INNOVATION MEETS REGULATION

Cybel Ekpa

A Comparative Analysis of Emerging Regulatory Frameworks

Abstract

The rapid proliferation of space technologies, from satellites and remote sensing platforms to commercial launch vehicles, has created an urgent need for robust, adaptable legal frameworks. This paper examines the intricate relationship between technological advancement and space law, using Nigeria's National Space Research and Development Agency (NASRDA) Act of 2010 as its primary lens. The paper explores how the Act's licensing mechanisms, regulatory institutions, and radio spectrum governance attempt to manage an increasingly technology-driven space sector. Through a comparative analysis with the United States Federal Communications Commission (FCC) under the Communications Act and the Federal Aviation Administration (FAA) under the Commercial Space Launch Act (CSLA) of 1984, the paper argues that space law is not merely a product of political will but is fundamentally shaped by, and responsive to, the technologies it seeks to regulate. The paper further identifies critical gaps in Nigeria's regulatory framework, including reliance on foreign launches, limited private-sector engagement, and aging satellite infrastructure. It proposes pathways for legal evolution aligned with contemporary technological realities.

Keywords: Space, Remote Sensing, Technology, Governance

Introduction

The history of space law is, at its core, the history of technology pressing against the boundaries of the existing legal order. From the moment the Soviet Union launched Sputnik in 1957, and the international community scrambled to establish norms for outer space conduct, the law has

perpetually chased technological development. Today, as commercial space activities grow exponentially, driven by reusable launch vehicles, satellite mega-constellations, and the ambitions of both state and non-state actors, the question of how law and technology interact in the space domain has never been more consequential.

Nigeria's National Space Research and Development Agency (NASRDA) Act of 2010 provides a compelling case study of a developing nation navigating this complex intersection. Founded in 1999 under former President Olusegun Obasanjo, NASRDA was established to develop a comprehensive strategy for space science and technology advancement (NASRDA Act, 2010). Over the following decades, Nigeria launched a series of satellites, NigeriaSat-1 (2003), NigComSat-1 (2007), NigeriaSat-2 and NigeriaSat-X (2011), and NigComSat-1R (2011/2012), and developed a legislative framework to govern the country's growing space activities (NASRDA, 2025; Space in Africa, 2021). As scholars such as Frans Von Der Dunk have observed, however, the NASRDA Act, while forward-thinking in its foundational structure, falls short in addressing specific operational intricacies essential for a thriving space sector (Von Der Dunk, 2011).

This paper interrogates the intertwining of technology and space law, examining the NASRDA Act's licensing regime, spectrum regulation, and comparative regulatory models. The analysis is organized around three central questions: How does technology drive the content and structure of space law? How do licensing frameworks operate as instruments of technological governance? And what systemic challenges arise when law fails to keep pace with rapidly evolving space technologies? By engaging these questions through both Nigerian and comparative U.S. perspectives, this paper contributes to a broader understanding of how emerging spacefaring nations can construct adaptive, technology-responsive legal frameworks.

Discussion

I. The Technological Foundations of Space Law

Space law is inherently technological in its origins and its evolution. The foundational international instruments governing outer space, the Outer Space Treaty of 1967, the Liability Convention of 1972, and the Registration Convention of 1976, were all direct responses to specific technological developments. The Outer Space Treaty, for example, was catalyzed by the technological shock of satellite launches and the need to prevent the weaponization of a new frontier (United Nations, 1967).

Each legal development followed a technological one, establishing a pattern that continues to define the discipline.

Nigeria's legislative trajectory mirrors this global dynamic. Before 1976, Nigeria had already expressed its intention to establish a comprehensive remote sensing center at an intergovernmental meeting in Addis Ababa, Ethiopia, recognizing the strategic importance of satellite data acquisition technology (NASRDA Center for Basic Space Science, n.d.). This led to the authorization of the National Center for Remote Sensing with its headquarters in Jos and a satellite ground receiving station at Kerang, near Panyan, Plateau State.

The passage of the NASRDA Act in 2010 was itself a legislative response to the technological reality of Nigeria's growing satellite portfolio. By then, Nigeria's portfolio included NigeriaSat-1, launched on September 27, 2003, as the country's first Earth-observation satellite, and NigComSat-1, launched on May 13, 2007, as Africa's first communications satellite, though NigComSat-1 failed in orbit in November 2008 due to a solar array anomaly and was subsequently de-orbited (Wikipedia –NigComSat-1, 2023; NIGCOMSAT, n.d.). Its replacement, NigComSat-1R, was launched on 19 December 2011 and delivered to orbit on 2 March 2012, following the passage of the Act (NASRDA, n.d.; AidData, n.d.).

The Act's definitional choices further illuminate the relationship between technology and law. By defining 'outer space' as any region beyond 100 km above sea level and a spacecraft launch as propelling an object to that altitude, the NASRDA Act anchors its legal concepts in measurable scientific parameters (Ekpa, 2024). This is not a trivial observation: legal definitions that are grounded in technological specificity are more effective at governing the activities they target than vague, technology-agnostic provisions. Such precision also facilitates compliance with international obligations under the Outer Space Treaty and the Registration Convention, both of which require that space objects be clearly identified and that states maintain jurisdiction over their space activities.

However, the technological foundations of Nigeria's space program also reveal significant vulnerabilities in its legal framework. Nigeria's satellites were purchased from foreign sources rather than developed domestically, and the country continues to rely on Chinese and Russian rockets for launch services (Center for Strategic and International Studies 2020). This dependency on foreign technology exposes a legislative gap: the NASRDA Act does not adequately address the regulatory complexities of international launch arrangements, technology transfer agreements, or the long-term strategic implications of a space program built on imported infrastructure. As noted by Ekpa (2024), Nigeria currently lacks an ongoing domestic launch system development program, and the technical challenges it faces are largely attributable to workforce competence gaps and insufficient training and retention structures for skilled professionals.

As of 2025, NASRDA has announced plans for an indigenous spaceport to be built around, 2025–2028 and aspirational targets to build satellites without foreign assistance (Wikipedia – NASRDA, 2025). Notably, in June 2025, Nigerian-born philanthropist Chief Owolabi Salis became the first Nigerian to travel to space, aboard Blue Origin's NS-33 mission, though this was a private rather than a government-backed undertaking (NASRDA, 2025). These developments do not resolve the legislative gaps identified in this paper but provide important forward-looking context for Nigeria's space trajectory.

II. Licensing as an Instrument of Technological Governance

Licensing regimes represent the most direct interface between space law and technology management. By conditioning access to space activities on compliance with regulatory requirements, licensing frameworks allow governments to shape the technological landscape of their national space sectors. In Nigeria, the NASRDA Act empowers the agency to issue licenses to individuals or corporate entities for activities specified under Section 6(k), which pertains to satellite data storage and management within Nigeria's territory (NASRDA Act, 2010). All partnerships or consultations regarding space data in Nigeria must be conducted via or with the agency, establishing NASRDA as the central regulatory hub for satellite data governance.

The draft regulations also establish a tiered licensing architecture for launch activities. A 'launch facility permit' authorizes the construction and operation of a launch facility in Nigeria, specifying the approved type of launch vehicle and designated flight paths. A 'launch permit' authorizes either a specific space object launch or a series of launches from a designated facility using a designated launch vehicle type. An 'overseas launch certificate' applies specifically to Nigerian nationals launching from foreign facilities, ensuring that the regulatory reach of the NASRDA framework extends beyond Nigerian borders. Finally, an 'exemption certificate' may substitute for any of these authorizations under specified circumstances (Ekpa, 2024). This layered system reflects the complexity of modern space operations, where a single satellite mission may involve multiple jurisdictions, technologies, and regulatory touch points.

The Nigerian Communications Commission (NCC), established under the Nigerian Communications Act of 2003, manages a parallel but complementary licensing regime for the radio frequency spectrum, a critical technological resource for all satellite operations. The NCC oversees spectrum auctions for cellular and fixed wireless access and is implementing a Spectrum Management and Monitoring System (SMMS) to improve radiofrequency governance (Nigerian Communications Commission Act, 2003). The SMMS requires telecommunications operators to provide

comprehensive information about their frequencies, equipment, and deployment sites, creating an updated frequency utilization database that facilitates interference resolution and spectrum planning. The NCC's licensing procedures are governed by principles of transparency, fairness, non-discrimination, and efficient spectrum management, as prescribed by Section 33(3) of the Nigerian Communications Act (2003).

Above the NCC in Nigeria's regulatory hierarchy sits the National Frequency Management Council (NFMC), housed under the Ministry of Information and Communications, which serves as the primary authority for coordinating radio spectrum allocation across all regulatory bodies, including the NCC and the National Broadcasting Commission (NBC). The NBC, in turn, licenses approximately 350 private, public, satellite, network, university, and community radio and television stations, and distributes apex authority frequencies to commercial and public broadcasters (Ekpa, 2024). This multi-layered institutional architecture, while comprehensive in scope, also creates potential for regulatory fragmentation, a challenge that technology-intensive industries such as space communications are particularly vulnerable to.

Comparing Nigeria's licensing framework to that of the United States illuminates both the strengths and limitations of the NASRDA model. In the United States, the FAA's Office of Commercial Space Transportation was originally established within the Department of Transportation in 1984 under the Commercial Space Launch Act and transferred to the FAA in November 1995 (FAA, 2025). The FAA issues launch licenses, reentry licenses, and launch site operator licenses and conducts safety inspections to ensure that commercial space activities do not pose undue risks to public health, property, or U.S. national security (U.S. Commercial Space Launch Competitiveness Act, 2015).

The FCC, operating under the Communications Act, manages spectrum allocation for satellite communications, coordinating with international bodies such as the ITU to ensure that U.S. satellite operators comply with global frequency coordination requirements. The U.S. framework reflects decades of regulatory refinement driven by technological change. As commercial

launch technology evolved, culminating in the development of reusable launch vehicles by companies such as SpaceX and Blue Origin, the regulatory framework was updated through the U.S. Commercial Space Launch Competitiveness Act of 2015 to accommodate new business models, streamline licensing processes, and reduce regulatory burdens on emerging commercial operators. Nigeria's NASRDA Act, enacted in 2010, has not yet undergone comparable updates, despite significant changes in the global space technology landscape over the intervening years.

III. Spectrum Regulation at the Technology-Law Interface

The management of the radio frequency spectrum represents one of the most technically demanding dimensions of space law. Satellites depend on specific frequency bands for command and control, telemetry, and data transmission, and the allocation of these frequencies involves both domestic regulatory decisions and international coordination through the International Telecommunication Union (ITU). Nigeria's licensing regulations require that licensees strictly comply with ITU regulations on the allocation of frequencies and orbital positions, embedding international technology standards directly into the national legal framework (Ekpa, 2024).

The ITU's Radio Regulations, which govern the global allocation and use of radio frequencies, are themselves a product of technological necessity. As satellite technology evolved and the number of operational satellites grew, the potential for radio frequency interference increased correspondingly, requiring ever more sophisticated international coordination mechanisms. Nigeria's compliance with ITU regulations is therefore not merely a matter of international legal obligation but a technological imperative: without adherence to ITU frequency coordination procedures, Nigerian satellites risk harmful interference from or to other operators, compromising their operational effectiveness.

The NCC's implementation of the SMMS further illustrates the interplay between technology and law in spectrum regulation. By collecting detailed data on frequencies, equipment, and deployment sites from telecommunications operators, the NCC is building the informational

infrastructure necessary for effective spectrum management in an increasingly congested radio environment. This data-driven approach to spectrum governance reflects a broader trend in space and telecommunications regulation toward evidence-based, technologically sophisticated oversight. This trend distinguishes advanced regulatory systems from their less developed counterparts.

IV. Systemic Challenges: When Law Fails to Keep Pace with Technology

The most significant dimension of the technology-law relationship in the space sector is regulatory lag, the tendency for legal frameworks to lag behind technological change. Nigeria's experience with its Earth-observation satellites provides a striking illustration. NigeriaSat-2 and NigeriaSat-X were launched on 17 August 2011 with a projected operational lifespan of seven years (through 2018). However, as of 2021, both satellites were reportedly still in orbit and operational, albeit not optimally, and had survived well beyond their design parameters (Oyewole, 2021; Space in Africa, 2021).

While this technological resilience might appear to be a straightforward success story, it also reveals a regulatory challenge: Nigeria's legal framework does not appear to have anticipated the operational, liability, and end-of-life implications of satellites operating beyond their projected lifespans.

While Section 9(4) grants discretionary authority to impose licensing conditions on payload disposal and contamination prevention, the Act lacks specific, enforceable standards. Unlike jurisdictions that mandate compliance with the Inter-Agency Space Debris Coordination Committee's 25-year deorbiting guideline or specify passivation procedures, Nigeria's framework leaves these critical operational requirements to ad hoc licensing decisions. As Nigeria's satellites age beyond their design life, this regulatory discretion creates uncertainty about liability allocation and debris mitigation responsibilities. (Von Der Dunk, 2011).

The absence of private sector engagement in Nigeria's space industry represents another critical regulatory challenge with deep technological implications. The Nigerian space industry is currently experiencing sluggish development due to a lack of private-sector engagement in commercial space activities (Ekpa, 2024). In contrast, the U.S. commercial space sector has flourished precisely because the regulatory framework, through the CSLA and subsequent legislative updates, has actively facilitated private investment, streamlined licensing, and created legal certainty for commercial operators. Nigeria's regulatory framework has not yet achieved this enabling function, in part because the NASRDA Act was designed primarily for a state-led space program rather than a mixed public-private space economy.

The contrast between Nigeria's state-centric model and the U.S. commercially oriented approach is instructive. The U.S. Commercial Space Launch Competitiveness Act of 2015 explicitly sought to encourage the development of a robust U.S. commercial space industry by reducing regulatory burdens and providing a more favorable legal environment for private investment. The Act also addressed novel legal questions raised by new space technologies, including the legal status of resources extracted from celestial bodies, an issue that no existing international space law instrument had previously addressed. Nigeria's legal framework, by contrast, has not yet engaged with these emerging technological and legal frontiers, reflecting a broader regulatory vision gap that must be addressed if Nigeria is to realize its space sector potential.

V. Toward an Adaptive, Technology-Responsive Space Law Framework

The foregoing analysis suggests that effective space law must not merely be reactive to technological change but proactively designed to anticipate and accommodate it. Several principles emerge from the comparative analysis of Nigerian and U.S. space regulatory frameworks that may guide the development of more adaptive legal instruments.

First, legal frameworks must be grounded in technological specificity. Vague or technology-agnostic legal provisions are poorly equipped to govern the complex operational realities of modern space activities. Nigeria's Act

benefited from its precise definitions of outer space and spacecraft launches; future legislative updates should extend this specificity to cover areas such as satellite end-of-life management, debris mitigation, and the regulation of emerging space technologies, including small satellites and on-orbit servicing vehicles.

Second, regulatory institutions must develop deep technological expertise. The NCC's implementation of the SMMS and its engagement with ITU frequency coordination processes reflect an institutional commitment to technology-informed regulation that other Nigerian space regulatory bodies should emulate. Building regulatory capacity through the recruitment of technically qualified staff, investment in monitoring and enforcement infrastructure, and active engagement with international technical standards bodies is essential for effective space governance.

Third, legal frameworks must create enabling conditions for private sector participation. The comparative success of the U.S. commercial space sector demonstrates that regulatory clarity, streamlined licensing, and legal certainty are prerequisites for attracting private investment in space activities. Nigeria's regulatory framework should be reformed to reduce administrative burdens on commercial space operators, provide clear legal pathways for new types of space activities, and establish a predictable, transparent regulatory environment that encourages entrepreneurial engagement in the space sector.

Finally, space law must engage actively with international legal developments. As the global space regulatory environment evolves, through updates to ITU regulations, the development of new norms for responsible space behavior, and the emergence of bilateral and multilateral agreements on space traffic management, Nigeria must ensure that its domestic framework remains aligned with international best practices. This requires not only compliance with existing international obligations but active participation in the processes through which new international norms are developed.

Conclusion

The relationship between technology and space law is not merely one of cause and effect but of continuous, dynamic interaction. Technology creates the conditions that space law must address; law, in turn, shapes the technological landscape by determining which activities are permitted, under what conditions, and by whom. Nigeria's NASRDA Act of 2010 represents a significant step in developing a national space legal framework, providing a foundational regulatory architecture for licensing, spectrum management, and compliance with international obligations. Yet, as this paper has demonstrated, the Act's provisions fall short in several critical areas, including satellite end-of-life management, private-sector facilitation, and domestic launch system development, that are essential to a viable, self-sustaining national space industry.

The comparative analysis with the U.S. FCC and FAA frameworks underscores the importance of regulatory adaptability and technological sophistication in effective space governance. The United States has repeatedly updated its space regulatory framework in response to technological change, creating a dynamic legal environment that has supported the emergence of a globally competitive commercial space sector. Nigeria must pursue a similar trajectory, committing to the ongoing review and reform of its space legal framework to ensure that it remains fit for purpose in a rapidly evolving technological environment.

The stakes of this regulatory evolution are high. Space technology offers transformative potential for Nigeria's development, in areas ranging from agriculture and natural resource management to disaster monitoring and communications connectivity. Realizing this potential requires a legal framework that is not only technically sound and internationally compliant but genuinely enabling: one that invites private investment, rewards innovation, and positions Nigeria as a confident and capable participant in the global space economy. The work of building such a framework is, at its core, ensuring that Nigeria's law keeps pace with its technological ambitions and

that those ambitions are bold enough to match the opportunities that space technology enables.

References

AidData. (n.d.). NigComSat-1 Communications Satellite Replacement Project. <https://china.aiddata.org/projects/1712/>

Center for Strategic and International Studies. (2020). Challenges and opportunities of Nigeria's space program. <https://aerospace.csis.org/challenges-and-opportunities-of-nigerias-space-policy/>

Daily Maverick. (2021, August 24). One of Nigeria's satellites is on its last legs. <https://www.dailymaverick.co.za/article/2021-08-24-one-of-nigerias-satellites-is-on-its-last-legs-why-this-is-worrying/>

Ekpa, C. N. (2024). An in-depth analysis of the National Space Research and Development Agency Act. ResearchGate. <https://doi.org/10.13140/RG.2.2.14153.31846>

Federal Aviation Administration. (2025). About the Office of Commercial Space Transportation. https://www.faa.gov/about/office_org/headquarters_offices/ast

International Astronautical Federation. (2025). National Space Research and Development Agency(NASRDA). <https://www.iafastro.org/membership/all-members/national-space-research-and-development-agency-nasrda.html>

International Telecommunication Union. (2020). Radio regulations. <https://www.itu.int/pub/R-REG-RR>

Mondaq. (2020, January 6). Nigeria: A brief review of NCC licensing regulations 2019. <https://www.mondaq.com/nigeria/licensing--syndication/880710/>

NASRDA. (n.d.). NigComSat-1R. <https://central.nasrda.gov.ng/space-missions/nigcomsat-1r/>

National Space Research and Development Agency Act. (2010). Federal Republic of Nigeria.

https://www.unoosa.org/documents/pdf/spacelaw/national/NASRDA_ACT_2010.pdf

Nigerian Communications Act. (2003). Federal Republic of Nigeria.

http://www.commonlii.org/ng/legis/num_act/ncca364/

Oyewole, S. (2021, August 24). One of Nigeria's satellites is on its last legs. Daily Maverick. <https://www.dailymaverick.co.za/article/2021-08-24-one-of-nigerias-satellites-is-on-its-last-legs-why-this-is-worrying/>

Resolution Law Firm. (n.d.). How to obtain an NCC license in Nigeria.

<https://www.resolutionlawng.com/how-to-obtain-ncc-license-in-nigeria/>

Sani, Y. M., & Sani Esq. (2022). Examining the regulatory regime for radio frequency spectrum licensing in Nigeria. ResearchGate, 10(2), 1–8.

https://www.researchgate.net/publication/378041549_Examining_The_Regulatory_Regime_For_Radio_Frequency_Spectrum_Licensing_In_Nigeria

Senate Report 114-88. (2015). U.S. Commercial Space Launch Competitiveness Act. <https://www.govinfo.gov/content/pkg/CRPT-114srpt88/html/CRPT-114srpt88.htm>

Mustapha Iderawumi. (2021, April 6). Replacing the Nigerian satellite past its design life: the journey so far - space in Africa. Space in Africa.

<https://spaceinafrica.com/2021/04/06/replacing-nigerian-satellite-gone-past-design-life-the-journey-so-far/>

SpaceNews. (2011, December 20). Nigcomsat-1R was launched successfully by Long March. <https://spacenews.com/nigcomsat-1r-launched-successfully-long-march/>

United Nations. (1967). Treaty on principles governing the activities of states in the exploration and use of outer space.

<https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspace treaty.html>

Von Der Dunk, F. (2011). The second African national space law: The Nigerian NASRDA Act. University of Nebraska–Lincoln.

<https://digitalcommons.unl.edu/spacelaw/92/>



TELEMEDICINE AND DATA PROTECTION CHALLENGES IN THE 21ST CENTURY

Christianah Akinyemi

Abstract

This work explored how the rapid evolution of the 21st century both contributed to the transformative development of telemedicine, enabling efficient provision of medical services through digital technologies, but yet exposed telemedicine to data protection risks in the face of many cybersecurity threats. The paper extrapolated the benefits and risks connected to this dual impact of technological advancement on telemedicine and provided strategies to mitigate them. Strikingly, the work underscored the need for robust regional and universal legal and regulatory frameworks to ensure cross border compliance and sustain telemedicine as an effective healthcare delivery model.

Introduction

One of the characteristics that marks the intersection between technology and medicine in the 21st century is the development of telemedicine, an invention that entails the provision of medical and care services at a distance with the aid of technology (Ansarian and Baharlouei, 2023). The medical services forged within the concept of telemedicine spread across consultation, patient monitoring, and transmission of health information, among others (Sud and Anjankar, 2022). Common to all these services is that they are provided remotely via technological apparatuses.

Telemedicine has largely sustained quality health care delivery, reducing time and connected costs, and curbing the spread of communicable diseases (Ansarian and Baharlouei, 2023). Despite its many benefits, the use of telemedicine comes with its own challenges, chief among which centers on the protection of medical information in light of the data protection scares peculiar to the 21st century. This particular risk gives rise to the need

for a robust legal and regulatory framework to sustain the safe use of telemedicine across the globe.

Against this backdrop, this work sets out to expound on telemedicine as a 21st century phenomenon, its benefits and risks, specifically elucidating on the data protection risks associated with the technology and chart effective legal and regulatory solutions as recommendations to ameliorate such risks.

Understanding Telemedicine in the 21st Century

Popularized during the COVID-19 pandemic of the year 2020 as the most effective means of health care delivery (Omboni et al., 2022), telemedicine has greatly developed on advanced digital technologies of the 21st century as a feasible and widely acceptable medical practice within the auspices of healthcare delivery (Pool et al., 2021). Prior to the 21st century, the concept of telemedicine was largely limited and experimental in nature. With early technologies like telegraph, radio transmissions and telephone, information exchange between health care providers and patients were facilitated as early as the 1900s, however being constrained by the limited capability for image transmissions, real time communications and high cost, telemedicine stayed limited and rare (Jagarapu and Savani, 2021).

The late 20th century as well as the 21st century has witnessed the advancement of telemedicine on the back of highly developed technologies (Gali, 2022). In current times, telemedicine now finds expressions across various practice areas within the medical and healthcare field including ophthalmology, psychiatry, dermatology, dentistry, respiration, emergency care and many other subfields in the medical field (Ansarian and Baharlouei, 2023). This wide spread and usage of telemedicine and its tools were significantly influenced by the Covid-19 pandemic in 2020. Current day technological devices used for telemedical purposes are likewise vast. They include: mobile applications, video conferencing, machine learning, wearable sensors, Internet of (medical) things and digital devices such as mobile phones and computers (Ansarian and Baharlouei, 2023).

In light of the foregoing, it can be gleaned that telemedicine has existed in rudimentary forms prior the 21st century, but its adoption was not largely improved and popularized until the 21st century, thanks to the development of information technology and the COVID-19 pandemic that hit the world as a shock wave, necessitating reduced physical contacts and the evolution of digital health.

The Benefits and Risks Associated to Telemedicine

Telemedicine offers many benefits to the healthcare systems, improving healthcare delivery and reducing healthcare practitioners' workloads. Significant among these benefits include:

- Accelerated access to medical practitioners at lower/affordable costs: telemedicine evaporates geographical barriers to accessing healthcare, enabling patients across various locales to consult medical professionals and care providers at the comfort of their homes, without the need for physical travel. This particular advantage is largely beneficial to patients resident in remote and underserved areas. Resultantly, telemedicine ameliorates costs that would have rather been expended on travels and other incurable costs (Gajarawala and Pelkowski, 2021).
- Reduction of the Workload of Healthcare Practitioners: telemedicine provides a convenient means for health care delivery. With the technological apparatuses, healthcare professionals can efficiently schedule appointments and effectively manage their time (Maddukuri et al., 2021).
- Telemedicine reduces the need for physical contacts, ameliorating the spread of contagious diseases and eases access to healthcare for vulnerable groups such as the elderly, pregnant women, physically disabled persons, among others (Wolf et al., 2022).

Notwithstanding these benefits, telemedicine also presents certain new risks, some of which ironically stem from the technological evolution of the 21st century. Telemedicine heavily relies on the exchange of data via digital platforms and tools. These platforms and tools are, however, susceptible to

data breaches and cyber attacks that may cause impacts such as unauthorized access, compromised confidentiality and the breach of data protection regulations (Chiang and Starren, 2021).

Apart from this, the dearth of physical examination characterizing telemedicine impedes accurate diagnosis and effective treatment (Bokolo, 2021), specifically for medical conditions that may require such examination. Nevertheless, telemedicine can be resorted to upon physical examination to complement treatment (Ansarian and Baharlouei, 2023).

Another factor that poses risk(s) to telemedicine is the uneven telemedicine access across locales and among persons. Remote areas are often plagued with inadequate technological infrastructures to support telemedicine (Gajarawala and Pelkowski, 2021). In the same vein, computer literacy and technological tools like smart phones, laptops and even the internet are not universally accessible among persons (Ansarian and Baharlouei, 2023), especially among the elderly, low income earners and persons residing in developing or underdeveloped locales. This disparity widens health inequalities, far from what telemedicine ordinarily seeks to represent.

Amongst the many risks telemedicine portends, this work narrows its focus on data protection risks, which arises as one of the most critical challenges in the 21st century delivery of healthcare services through telemedicine. This is necessary as data protection has far reaching legal, regulatory and ethical implications, adequately interweaving the law with the healthcare sector.

Data Protection Risks: Impacts on Telemedicine

The 21st century technological innovations come with certain data protection risks that affect the use of technology across various industries, including the healthcare sector. This subhead sets out these possible risks with their implications on the use of technology in rendering healthcare services.

- **Unauthorized Access and Interceptions:** certain telemedicine platforms are not well encrypted enough to protect against unauthorized access to the personal and health information (PHI) of patients. This risk can

potentially lead to data breaches and puncture patients' trust in telemedicine (Ritunga et al., 2025).

- **Device and Network Vulnerabilities:** patients or practitioners' devices and their respective networks where susceptible to vulnerabilities such as phishing, malware and personal data theft, open the personal and health information of patients to breaches.
- **Cyber and Malware Attacks:** the prevalent cyber attacks leveled against the healthcare sector are ransomware and cryptojacking (Cybersecurity National Coordination Center Malta, 2021). Ransomware infects servers by maliciously encrypting any data it finds and demands an online payment to get the password to decrypt. This cyber attack has been targeted against many healthcare facilities. Good examples are the ransomware attacks against the Illinois Public Health Website and a medical testing facility in the UK (Jalali et al., 2020). Cryptojacking on the other hand is much more covert; it wears down targeted systems to mine cryptocurrency and can also be used to infuse ransomware.

The implications of these risks are far reaching. It includes financial loss and penalties, for instance the US Health Insurance Portability and Accountability Act, which provides certain standards to protect the personal and health information of patients, sets significant fines for non-compliance (Holt, 2025). Some other impacts include patients' loss of confidence in telemedicine, lawsuits and reputational damages.

Extant Data Protection Legal Frameworks and their Impact on the Development of a Telemedicine Policy

Health information occupies a privileged and sensitive category of data across various data privacy frameworks, accorded heightened protection under the GDPR and protected as highly sensitive information across other jurisdictions. Its protection also formed the basis for the development of HIPAA. On the other hand, telemedical services, by their very nature, largely rely on the storage, transfer and real time processing of health information, more so, on a large scale, across devices, technological platforms, borders

and jurisdictions. It is therefore imperative that a proper telemedicine policy aligns with the established standards protected by these data privacy laws across jurisdictions.

This is important as reliance on telemedical services have generally raised questions among scholars, regarding the exact data protection law that would apply in data privacy matters arising from cross-border interactions between patients and healthcare providers using telemedical platforms to render health care services (Bensemmane and Baeten, 2019). While the determination of this question would warrant practitioners to navigate a complex web of regional regulations, national data privacy laws and licensing frameworks, this article holds that these legal regimes all have in common, certain established privacy standards which they uphold and protect, and which a well-designed telemedicine policy must reflect.

In light of the foregoing, this subheading draws on two dominant data protection frameworks, including the United States' Health Insurance Portability and Accountability Act (HIPAA) and the European Union's General Data Protection Regulation (GDPR), examining their direct implications for telemedicine practice, thereby extrapolating the principles that could form the core components of a Telemedicine Policy.

JOURNAL OF IP PROFESSIONALS

The United States' Health Insurance Portability and Accountability Act (HIPAA) represents a data protection legislation that is sector specific, protecting patients' health information from data privacy breaches. Recognizing the legal force of this legislation, the Office of Civil Rights (OCR) gave a directive, mandating the compliance of telemedical services with the provisions of HIPAA, including switching to a HIPAA-compliant telehealth vendor (Fortinet, 2026).

The rules under the HIPAA Framework can be categorized as Privacy Rule and Security Rule, and they both apply to all modes of healthcare service delivery, whether done remotely or face to face (HIPAA Journal, 2026). Per the privacy rules, health practitioners are to obtain patients' consents before using or disclosing their Protected Health Information. More specific to telemedical health services, practitioners will therefore be obligated to verify

the identity of patients hosted on remote facilities; and request consent to proceed where the patient is with a third-party, such as a caregiver or a family member, and when the patient is in a public place where consultation might be overheard (HIPAA Journal, 2026). This obligation can be clearly incorporated into a telemedicine policy.

Security rules go further to ensure protection against impermissible and inadvertent disclosure or violation of the provisions of HIPAA, inculcating all available physical, administrative and technical safeguards. Narrowing it down to telemedicine services, health practitioners must only use approved HIPAA-compliant platforms, such as Amwell, athenaOne, Doximity, among others (Fortinet, 2026). These platforms provide necessary encryption to safeguard against cybersecurity risks such as data interception, unauthorized access, among others. Likewise, the HIPAA warrants software vendors to enter into Business Associate Agreement(s) with healthcare providers, as they both have persistent access to the protected health information passing through or stored on the servers of telemedicine platforms (HIPAA Journal, 2026). All these obligations can be replicated and further developed in a comprehensive telemedicine policy.

Another obligation which comes under the security rule and may be replicated in a telemedicine policy is the requirement of periodic risk assessments, to detect and solve cybersecurity risks in line with established cybersecurity standards, such as the NIST standards.

Moving on to the EU's General Data Protection Regulation, this legislation holds some extraterritorial reach, it applies as long as the data subject resides in the EU, notwithstanding where the processor or controller is headquartered (Eikelder, 2026). In the parlance of personal health data, the legislation has been viewed by scholars as one that provides a more comprehensive response to issues that challenge the protection of health data (Malgieri and Comandé, 2017; Yuan and Li, 2019). It accords patients with more rights and power in the control and ownership of their health information and toughens the data protection responsibilities of controllers and processors (Yuan and Li, 2019).

To be specific, under the EU GDPR, health information is classified as a special category data and accorded the highest tier of protection (Article 9). The legislation generally prohibits its processing, except it is processed on any of the bases set out in Article 9(2) and Article 6 of the legislation. Furthermore, due to the large sets of health information processed on telemedicine platforms, such platforms and systems must comply with the Data Protection Impact Assessment (DPIA) requirement under Article 35, which is necessary to identify possible risks associated with processing done through new technologies and ameliorate them before embarking on processing such information. This requirement is a pivotal one for telemedicine policy to model after.

In addition, just as required under HIPAA, software vendors must enter into data processing contracts under Article 28 of the GDPR, ensuring the legal accountability of these vendors for the data they store and process on behalf of healthcare providers. The GDPR also obligates data controllers and processors to implement appropriate technical and organizational measures to safeguard the information in their care (Arts 25 & 32). In the context of telemedicine service, such measures would cut across encryption, access controls, intrusion detection systems, among others, and it is necessary that they are clearly spelled out in a telemedicine policy.

In conclusion it is apposite to note that, the GDPR provides for certain rights which are accessible to patients (data subjects) in the context of telemedicine service. They include: the right to be informed of possible data privacy risks in an intelligible and easily accessible form, using clear and plain language under Article 7; the right to access the health information held of them, which must be granted in 30 days upon request (Arts 12 and 15); the right to transfer their health data from one controller to another without hindrance from the former (Article 20); and the right to seek the erasure of the health information held of them (Article 18); The legislation also educates data subjects (patients) on the intricacies of automated processing, a central characteristic of telemedicine platforms, including their associated risks and consequences (Articles 12, 13, 22, 29). All these can indeed be largely instructive for designing a comprehensive telemedicine policy.

Jurisdictional Conflicts in Cross-Border Telemedicine Services

Perhaps there is no issue as more complex in the parlance of cross-border Telemedicine Practices than the challenge of jurisdiction. This challenge comes in a cluster of overlapping questions including: which country's licensing rules govern the doctor? Which data protection law governs the Patient's health data? Which court has the jurisdiction to resolve conflict if they arise?

In the US, jurisdictional conflicts may take two forms. First, the domestic form, which arises from the fact that the regulation of medical practice in the country is determined by each respective States, as such, a medical practitioner can only practice in the State(s) where they are licensed. Telemedicine challenges this principle due to its cross-border nature. As a result, where a medical practitioner licensed in Texas renders healthcare services through a telemedicine platform, to a patient domiciling in New York, such practitioner has in the strict sense of the law practiced in New York without a license.

This challenge was temporarily addressed during the COVID-19 pandemic, with resort to emergency waivers that allowed doctors in the US to practice across State jurisdictions. However, these waivers have expired since May 2023 (U.S. Department of Health and Human Services, Assistant Secretary for Planning and Evaluation [ASPE], 2024). Another temporary solution came with the Interstate Medical Licensure Compact (IMLC), which allows a medical practitioner practice in over 35 States in the US through a single license. Nevertheless, this hasn't precluded States from issuing, renewing and regulating the issuance of medical licenses independently (Ivanova, 2026).

The other aspect is transnational in nature, and it affects both the US and every other jurisdiction across the globe. Cross-border telemedicine service naturally invokes the applicability of a large body of laws, regulating all aspects of telemedicine services including market access, contracts, software developer's liability, data protection and court jurisdiction, making it impossible for a single extant law to regulate all aspects of telemedicine. For

instance, under the EU Private International law, matters arising from a breach of contract of this nature, in the absence of a choice of law agreement, will be governed by the law of the service provider's habitual residence (Rome I Regulation). However, this differs from the provisions of the EU GDPR on the subject of data protection, which will apply in all possible situations affecting EU residents.

In addition to this, many countries are yet to situate telemedicine on a statutory or regulatory framework, let alone formulate rules that would define the situations where a foreign medical practitioner may be allowed to treat her citizens (Lovells, 2020). This opens a lot of possibilities for risks such as the inadvertent violation of foreign medical licensing laws/regulations, dearth of legal reliefs for patients and cross-border enforcement limitations.

It is the argument of this exegesis that all these challenges can be sorted by specific telemedicine policies both in the international and national scenes, such policy would consolidate all the multi-dimensional areas affecting telemedicine service such as licensing, jurisdiction, data protection, market access, developer's liability, among others, which are currently being regulated by different bodies of laws.

Risk Mitigation Strategies and Recommendations

Mitigating data protection risks in the context of telemedicine requires a multifaceted approach. The first step involves training healthcare professionals on the procedures necessary to uphold patient privacy while engaging technological devices for healthcare services and informing patients on data collection methods with their associated risks (Ritunga et al., 2025). In the same vein, healthcare organizations should amplify security systems with advanced encryption protocols, multi factor authentication and strong identity systems. They should also put in place advanced security systems and risk assessment procedures to identify vulnerabilities such as software in need of upgrade or patching and create comprehensive and proactive response plans and systems. Another step to be taken towards risk mitigation is facilitating international and regional cooperation on developing and ensuring compliance to policies and standards for telemedicine. Such

policies can be modeled after established ones like the NIST, GDPR and HIPAA. With this, the international community will be on the same page, harmonizing standardized protocols for telemedicine, ensuring cross-border compliance and harmonizing all multi-dimensional areas of law arising from telemedicine service.

Conclusion

Technological innovation of the 21st century offers telemedicine a significant shift, contributing to improved healthcare delivery and reach. However, this development likewise presents certain challenges, chief of which is data protection risks. This work examined the risks and advanced recommendations to ameliorate them, ultimately preserving telemedicine as a viable and effective means of healthcare delivery.

References

- Ansarian, M., and Baharlouei, Z. (2023). 'Applications and Challenges of Telemedicine: Privacy-Preservation as a Case Study.' *Archives of Iranian Medicine*, 26(11), 654-661.
- Bensemmane, S., and Baeten, R. (2019). 'Cross-border telemedicine: practices and challenges.' OSE Working Paper Series, Research Paper No.44 Brussels: European Social Observatory,
- Bokolo, A.J. (2021). 'Application of telemedicine and eHealth technology for clinical services in response to COVID-19 pandemic.' *Health and Technology*, 11(2), 359–366.
- Chiang, M.F., Starren, D.G. (2021). 'Computer Applications in Health Care and Biomedicine.' Springer International, 667–692.
- Cybersecurity National Coordination Center Malta. (2021). 21st Century Healthcare Industry Cyber Protection Challenges 25 April, Available at: <https://ncc-mita.gov.mt/articles/21st-century-healthcare-industry-cyber-protection-challenges/> (Accessed 15 January 2026).

Eikelder, M. (2026). Requirements for Transferring Patient Data Across Borders 4 March, Available at: https://www.kiteworks.com/hipaa-compliance/healthcare-data-sovereignty-cross-border-transfer/#GDPR_The_European_Layer (Accessed 4 June 2026).

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Fortinet. (2026). 10 Best HIPAA-Compliant Telehealth Platforms, Available at: <https://www.fortinet.com/uk/resources/articles/hipaa-compliant-telehealth-platforms> (Accessed 4 June 2026)

Gajarawala, S.N., and Pelkowski, J.N. (2021). 'Telehealth benefits and barriers.' *The Journal for Nurse Practitioners*, 17(2), 218–221.

Gali, C. (2022). History of Telemedicine (Curogram Blog) 2 August, Available at: https://curogram.com/blog/history-of-telemedicine?hs_amp=true (Accessed 13 January 2026).

Holt, D. (2025). The Legal Implications of Data Breaches in Telemedicine: Lessons Learned (Holt Law) 19 February, Available at: <https://djholtlaw.com/the-legal-implications-of-data-breaches-in-telemedicine-lessons-learned/> (Accessed 15 January 2026).

HIPAA Journal. (2026). HIPAA Guidelines on Telemedicine, Available at: <https://www.hipaajournal.com/hipaa-guidelines-on-telemedicine/> (Accessed 4 June 2026).

Ivanova, J. (2026). Telehealth Licensure 2025–2026: Cross-State Practice and Compacts 5 January, Available at: <https://telehealth.org/news/telehealth-licensure-2025-2026-cross-state-practice-and-compacts/> (Accessed 4 June 2026).

Jagarapu, J., and Savani, R.C. (2021). 'A Brief History of Telemedicine and the Evolution of Teleneontology.' *Seminars in Perinatology*, 45(5).

Jalali, M.S., Landman, A., and Gordon, W.J. (2020). 'Telemedicine, Privacy and Information Security in the Age of COVID-19.' *Journal of the American Medical Informatics Association*, 28(3), 671.

Lovells, H. (2020). International Telemedicine: A Global Regulatory Challenge 9 March, Available at: <https://www.lexology.com/library/detail.aspx?g=f2d9946b-e5c3-43f5-b813-9528e23afbda> (Accessed 4 June 2026).

Maddukuri, S., Patel, J., and Lipoff, J.B. (2021). 'Teledermatology addressing disparities in health care access: a review.' *Current Dermatology Report*, 10(2), 40–47.

Malgieri, G. and Comandé, G. (2017) 'Sensitive-by-distance: Quasi-health data in the algorithmic era.' *Information & Communications Technology Law*, 26, 229–249.

Omboni, S., Padwal, R.S., Alessa, T., Benczúr, B., Green, B.B., and Hubbard I. (2022). 'The worldwide impact of telemedicine during COVID-19: current evidence and recommendations for the future.' *Connect Health*, 1, 7–35.

Pool, J., Akhlaghpour, S., and Fatehi, F. (2021). 'Health data privacy in the COVID-19 pandemic context: discourses on HIPAA.' *Studies in Health Technology and Informatics*, 279, 70–77.

Ritunga, I., Harsa, C., Santoso, J., Nuhardi, M.S., Nugraheni, E., Peritiwi, S.I., and Alkatiri, N.S. (2025). 'Privacy and Confidentiality in Telemedicine: a Literature Review.' *Christian Journal for Global Health*, 12(1), 74-82.

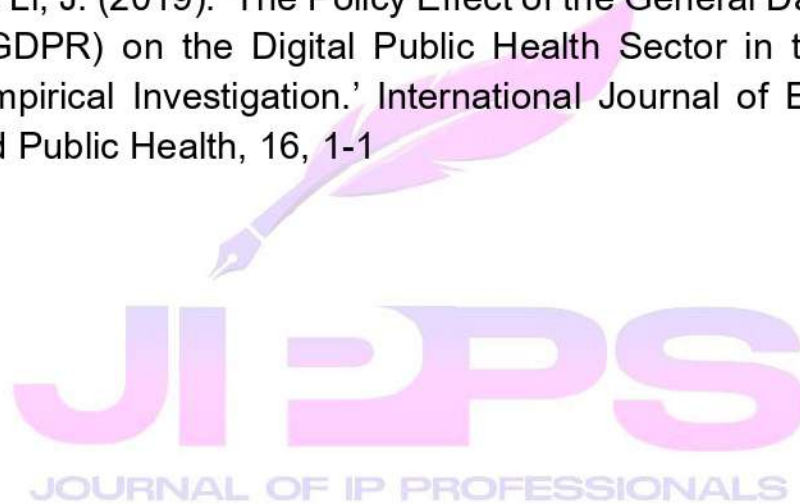
Sud, E., and Anjankar, A. (2022). 'Applications of Telemedicine in Dermatology.' *Cureus*, 14(8).

U.S. Department of Health and Human Services, Assistant Secretary for Planning and Evaluation [ASPE]. (2024). *Barriers and Opportunities for*

Improving Interstate Licensure Reciprocity and Portability for Behavioral Health Practitioners: Technical Expert Panel Findings 1 August, Available at: <https://aspe.hhs.gov/sites/default/files/documents/405ad876b1de337a81b4db0257666586/barriers-opportunities-improving-interstate-licensure.pdf> (Accessed 4 June, 2026)

Wolf, T.G., Schulze, R.K., Ramos-Gomez, F., and Campus, G. (2022). 'Effectiveness of telemedicine and teledentistry after the COVID-19 pandemic.' *International Journal of Environmental Research and Public Health*, 19(21).

Yuan, B., and Li, J. (2019). 'The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation.' *International Journal of Environmental Research and Public Health*, 16, 1-1



BRIDGING THE DATA DIVIDE: HOW THE UNITED STATES CAN SHAPE NIGERIA'S DIGITAL TRADE FUTURE.

Blessing C. Jones

Abstract

This article examines the regulatory misalignment between the United States and Nigeria in the areas of digital trade, data protection, and cross-border data governance, and analyzes how these disparities affect bilateral digital commerce and investment. As Nigeria's digital economy expands—particularly in fintech, e-commerce, and creative industries—regulatory fragmentation in privacy standards, cybersecurity obligations, data-localization expectations, and digital taxation increasingly constrains cross-border collaboration with U.S. firms, the country's largest source of foreign digital investment. The study reviews recent legal and policy developments, including Nigeria's Data Protection Act and the General Application and Implementation Directive (GAID) 2025, alongside evolving U.S. digital trade positions, California-led privacy standards, and the NIST Cybersecurity Framework. Through comparative regulatory analysis, the article identifies key structural gaps that raise compliance costs, delay partnerships, and discourage innovation. It proposes targeted harmonization strategies—such as adequacy determinations for cross-border data transfers, tiered audit thresholds, mutual recognition of cybersecurity standards, and calibrated digital tax exemptions—to reduce friction without undermining national sovereignty. The article concludes that strategic regulatory alignment can unlock significant trade potential, enhance investor confidence, and position Nigeria as a trusted hub in the global digital economy.

Introduction

Digital trade has emerged as one of the most consequential drivers of economic growth in the twenty-first century, reshaping how nations exchange goods, services, and information across borders. For Nigeria, the largest digital economy in Africa, this transformation is most visible in the rapid expansion of fintech services, e-commerce platforms, and digital

creative industries. The United States plays a central role in this growth trajectory, serving as the leading source of foreign digital investment and technological infrastructure. Yet, despite the strong commercial ties between the two countries, regulatory divergence in data governance and digital trade policy increasingly threatens to slow the momentum of this partnership.

At the core of the challenge lies a mismatch in data protection standards, cybersecurity obligations, cross-border transfer rules, and digital taxation frameworks.

Nigeria's regulatory architecture has undergone substantial reform in recent years, particularly with the enactment of the Nigeria Data Protection Act and the issuance of the General Application and Implementation Directive (GAID) 2025, which introduced stricter compliance requirements and heightened scrutiny of international data flows. Meanwhile, the United States continues to operate under a decentralized privacy regime characterized by state-level legislation, voluntary cybersecurity standards, and evolving digital trade commitments embedded in bilateral and multilateral agreements. The absence of a unified federal privacy statute and shifting trade positions create uncertainty for Nigerian firms seeking predictable regulatory pathways for U.S. partnerships.

JOURNAL OF IP PROFESSIONALS

The regulation of digital trade and data governance is increasingly shaped by the interplay of national legal systems and international frameworks. In examining the regulatory misalignment between Nigeria and the United States, this paper adopts a comparative regulatory analysis grounded in established theories of international trade law and regulatory governance. Specifically, the analysis is informed by mutual recognition theory, which explores how jurisdictions acknowledge and accept each other's regulatory standards to facilitate cross-border transactions, and the literature on regulatory convergence, which examines the processes and challenges of harmonizing legal regimes in the digital economy.

Furthermore, this Paper draws on international regulatory cooperation models, which provide insights into how states negotiate, implement, and sustain collaborative arrangements in the face of divergent policy objectives

and asymmetrical power relations. This theoretical lens enables a nuanced understanding of the structural barriers to regulatory alignment, the legal and political implications of harmonization, and the potential for mutual recognition or equivalence determinations as alternative pathways. By situating the analysis within these scholarly traditions, the paper seeks to contribute to the broader discourse on digital trade governance, moving beyond descriptive policy analysis to engage with the systemic and conceptual dimensions of regulatory cooperation in the digital age. This approach not only clarifies the analytical foundations of the study but also positions its findings within the ongoing debates on data localization, digital constitutionalism, and the political economy of U.S.–Nigeria trade relations.

U.S. and Nigeria's Digital Trade Policy and the Governance Gap

The rapid growth of digital technologies in the United States in recent years has created new opportunities for U.S. consumers and businesses but also new challenges in international trade. For example, consumers today access e-commerce, social media, telemedicine, and other offerings did not imagine thirty years ago. Businesses use advanced technology to reach new markets, track global supply chains, analyze big data, and create new products and services (Congressional Research Service, 2021). New technologies have been known to facilitate economic activity. Data and data flows have become a pillar of innovation and economic growth. According to the Department of Commerce, digital economy accounted for 9.6% of U.S. gross domestic product (GDP) in 2019 and supported 7.7 million U.S. jobs, or 5.0% of total U.S. employment in 2019. From 2005 to 2019, real value added for the U.S. digital economy grew at an average annual rate of 5.2% per year, outpacing the 2.2% growth in the overall economy each year (US. Bureau of Economic Analysis, 2021)

Given these statistics, the United States spends nearly 60 percent of all fintech investment in Nigeria, making it the biggest foreign money source in Africa's largest digital economy. Nigeria's fintech sector hit \$1.13 billion in 2024. (IMARC Group, 2024). The sector is projected to grow 15.82% each year through 2033 (IMARC Group, 2024), while e-commerce should reach

\$16.83 billion by 2030 (B2C E-Commerce Market Report, 2026). However uncertain these projections may seem, the regulatory misalignment between Nigerian and U.S. data protection frameworks needs an overhaul as it imposes compliance costs that inhibit cross-border digital commerce.

Countries have been working to build a governance framework to promote digital trade. The digital trade governance system involves both a country's national regulations and international agreements between countries. The number of trade agreements involving e-commerce or digital trade governance is increasing. As of June 2022, 138 trade agreements contained digital trade or e-commerce clauses (Burri et al., 2022). Technically, trade agreements are usually focused on reducing or eliminating traditional trade barriers such as tariffs and quotas. However, as time passed, the scope of trade agreements and policies have broadened to include cooperation on several non-trade issues, such as regulatory policies. An important form of cooperation in this area is harmonization of product standards (Maggi & Marazova, 2024). Harmonization involves creating uniform standards across countries to facilitate trade and ensure consistency in regulations. All these reports and theories form a simple efficiency rationale for harmonization, if products need to comply with different regulations across markets, companies will have to incur extra costs of certification, product specifications and information acquisition, and these are generally considered to be fixed costs. Hence one pays compliance costs from time to time, and these extra costs are not related to the products or services being traded (Lamy, 20215). Now, should trade policies push governments to harmonize standards, or rather encourage them to diversify standards? With Digital Trade on the rise, this should be investigated and resolved.

In Nigeria, President Bola Tinubu signed the Nigeria Data Protection Act into law, scrapping the five-year-old regulation previously in force (IDO, Ogele & Akintola, 2023). Nigeria's data protection setup began to change dramatically in September 2025. The General Application and Implementation Directive (GAID) 2025, replaced the old Nigerian Data Protection Law, bringing in more stable rules for moving data across borders. Digital Trade Governance gap creates real barriers for U.S. companies and

Nigerian businesses to work together. The alignment of these standards is not simply procedural; it is the critical foundation for unlocking billions in trade and investment between the two countries.

To bridge the governance gap between the U.S and Nigeria and practically other countries, we must consider the proponents of harmonization, mutual recognition, and equivalence determinations in international trade law:

- Harmonization focuses on creating uniform standards across countries to facilitate and encourage trade and promote consistency in trade regulations by different countries.
- Mutual Recognition allows countries to accept each other's regulations and standards as valid, even where they differ, promoting trade without requiring uniformity.
- Equivalence Determinations helps countries and trade organizations assess whether different regulatory measures achieve the same goals, allowing for trade based on comparable safety or quality levels rather than bias.
- Trade Facilitation: Harmonization aims for seamless trade through uniformity, while mutual recognition and equivalence focus on flexibility and acceptance of diverse standards.
- Regulatory Autonomy: Mutual recognition and equivalence allow countries to maintain their regulatory autonomy while still engaging in international trade.

Nigeria's Data Protection and Digital Regulations

Over the years, Nigeria has developed a legal framework to protect data privacy, aligning with global standards such as the EU's GDPR. For example, the Nigeria Data Protection Act 2023 (NDPA) was specifically enacted to safeguard personal information and implement data protection nationwide. In June 2023, The Act set up the Nigeria Data Protection Commission as an independent body with stronger enforcement powers than the National Data

Protection Bureau had (IDO, Ogele & Akintola, 2023). On September 19, 2025, the Commission rolled out the General Application and Implementation Directive 2025 (Osundolire, Aguocha, Hassan, 2025). This officially ended the 2019 Nigeria Data Protection Regulation and ushered in stricter compliance requirements as demanding as the GDPR but tailored to African needs.

GAID 2025 groups organizations into Data Controllers or Processors of Major Importance. This depends on how much data they consume and how sensitive it is. For example, Ultra-High-Level companies that have been known to process data from more than 50,000 individuals, pay one million naira in annual registration fees and must finish their first data protection audits within 15 months (Oyebode, 2025). Also, in August 2025, the Commission issued a public notice announcing the commencement of sector-by-sector investigations into companies suspected of non-compliance with the provisions of the Nigeria Data Protection Act 2023 (NDPA) (Ogele and Akintola, 2025). These companies have 21 days each to show they are compliant or risk fines and prosecution.

Cross-border data transfers have special focus on the new rules. Schedule 5 of GAID lays out two main paths: (1) send data to countries the Commission calls "adequate" on data protection or (2) use Cross-Border Data Transfer Instruments like standard contractual clauses. Nigeria hasn't published an adequacy list yet, so companies must fall back on contracts and explicit consent. The Commission kept the power to demand prior approval for sensitive transfers. That adds delays to deals with U.S. cloud providers, which is where most Nigerian data reside right now.

Digital taxation has also become a source of revenue for the Nigerian economy. The Federal government receives Value-Added-Tax from non-resident digital service providers in 2020 after amending Section 10 of the VAT Act. By September 2025, the Federal Inland Revenue Service had pulled in over six hundred billion naira from Facebook, Amazon, Netflix, and others (Adeyemi, 2025). Google, Microsoft, and TikTok have remitted almost three trillion naira in taxes alone in just the first half of 2024 (Adeyemi, 2025).

Beginning from January 2026, non-resident providers earning more than \$25,000 a year from Nigerian customers must register through a Simplified Compliance Regime portal and charge 7.5% VAT on all digital services (Asquith, 2025).

Cybersecurity regulation comes from several laws. Cybercrime (Prohibition, Prevention, etc.) Act 2015 provides that companies must report breaches to the Nigerian Computer Emergency Response Team within seven days or get hit with ten million naira in fines and seven years (Scoop, 2025). The Nigerian Communications Commission, supported by World Bank, is writing a telecommunications-specific cybersecurity framework due in 2026. This will target telecom operators with incident management and risk assessment standards. All this responds to Nigeria getting hit with 6,101 cyberattacks weekly in 2025, the worst in Africa (Bewa, 2025).

Key Differences Between Nigerian and U.S. Rules

When Nigerian fintech companies try to team up with U.S. payment processors or e-commerce platforms that use American cloud services, they encounter regulatory setbacks. Nigeria's GAID ensures Ultra-High-Level data controllers, companies consuming data from over 50,000 people, complete full audits and pay one million naira annually (Oyebode, 2025). Comparatively, California's Consumer Privacy Act works differently. It hits businesses with annual revenues of over \$25 million or those processing data for over 50,000 residents. There's no audit fee, but companies must do biennial assessments and file privacy impact reports for risky automated decision-making. Nigerian firms pay more up front whereas U.S. companies deal with ongoing compliance burdens.

Cross-border transfer rules don't match up either. GAID only allows transfers to "adequate" jurisdictions or through approved contractual clauses. Nigeria hasn't published any adequacy determinations yet. Under USMCA, the U.S. and its partners must permit unrestricted data flows, no localization requirements, no prior approvals. Nigerian companies using U.S. cloud infrastructure get stuck waiting for case-by-case approvals. Projects can be delayed for up to 60 days.

Nigeria's Cybercrimes Act requires breach reporting within seven days, or you face fines up to ten million naira and 7 years in prison (ibid., 2025). Whereas the United States has no comprehensive national breach-reporting statute, relying instead on sector-specific instruments such as HIPAA and SEC disclosure guidance. This fragmented approach produces conflicting compliance obligations for multinational firms operating across both jurisdictions.

Digital taxation is another flashpoint. Nigeria's 7.5% VAT on non-resident digital services kicks in above \$25,000 in annual revenue and brought in six hundred billion naira (Adeyemi, 2025). Most U.S. digital services taxes are one-sided moves. Congress has warned it might slap retaliatory tariffs on countries with DSTs, Nigeria included. That raises the risk of back-and-forth trade fights. These gaps in privacy rules, data flows, security standards, and tax policy slow down U.S. investment and create headaches for Nigerian exporters. The argument for targeted harmonization is hard to ignore.

Compliance Burdens and the Cost of Regulatory Divergence

For Nigerian digital companies seeking for U.S. partnerships, regulatory complexity has gone from annoying to life-threatening. In April 2025, the Central Bank of Nigeria hit Paystack with a two hundred and fifty million naira fine for running its Zap product without the right license (Wyne-Ng, 2025). This wasn't about fraud, but about having unclear rules about whether Zap was a wallet service or payment processor. Between October and December 2024, CBN handed out over ₦15 billion penalties to banks for compliance slip-ups. That pressure rolled downhill to fintech partners, who now face threats about license seizure if the sponsoring Banks draw regulatory heat.

Fintech firms are now directing between 15 and 25 percent of their operating budgets toward compliance infrastructure—expenditure that displaces product development investment. The tightening of the breach reporting window to 72 hours in 2024 requires continuous monitoring capabilities that smaller firms are often unable to sustain financially. Firms processing data relating to more than 50,000 individuals must complete data protection audits within 15 months and pay one million naira in annual registration fees. U.S.

platforms that are hosting Nigerian data don't pay these costs (Oyebode, 2025).

E-commerce platforms run into friction, moving money across borders. Sending payments within Africa can eat up 9% of transaction value, versus a global average of 6.3% (Duplo, 2025). Currency swings make it worse. Nigerian merchants using Stripe or PayPal watch their margins disappear as the naira-to-dollar rate shifts between when a customer orders and when the payment settles. Intra-African trade accounts for just 15% of the Continent's total commerce, 60 percent for European nations, mostly because payment infrastructure can't keep up with how fast digital commerce moves (Ibid., 2025).

The creative industries present a distinct but equally consequential set of regulatory challenges. Nigeria's Copyright Act 2023 modernised digital content protections, yet it left unresolved gaps concerning cross-border licensing terms applicable to streaming distribution. Nigerian musicians and filmmakers licensing their work to platforms such as Spotify or Netflix are compelled to negotiate under contractual frameworks that do not account for Nigeria's data residency requirements or applicable withholding tax obligations. These gaps are further complicated by the emergence of AI-assisted content creation: as over 60% of African creatives employ artificial Intelligence tools in content production, questions of intellectual property ownership and the applicable cross-border licensing framework become correspondingly more acute and legally uncertain (Ajayi, 2025).

These compliance burdens do not merely constrain growth; they redirect it. Nigerian digital firms gravitate toward markets offering greater regulatory clarity, while U.S. partners demonstrate increased reluctance to enter arrangements encumbered by poorly understood and asymmetric compliance obligations.

Toward Regulatory Alignment: Analytical Framework for Policy Reform

Nigeria can fix these regulatory gaps without giving up control over its data. That would put it at the center of U.S. digital investment into Africa.

1.First, the NDPC should publish draft adequacy standards by Q2 2026, calibrated to align with the USMCA framework's treatment of cross-border data flows. The United States does not require prior approval for outbound data transfers; Nigeria could adopt a functionally equivalent mechanism by establishing an expedited adequacy list, encompassing the United States, Canada, and Japan as initial designations, within a twelve-month timeframe. This would enable Nigerian fintech firms such as Opay and Paga to utilize U.S. cloud infrastructure without incurring the case-by-case prior-approval delays that currently extend to approximately 60 days per transaction.

2.Second, compliance costs should be recalibrated through the introduction of a tiered audit system: entities handling fewer than 10,000 records would be exempt from mandatory audit requirements, while those processing between 10,000 and 50,000 records would be subject to biennial rather than annual review. This approach brings Nigeria's framework into closer

alignment with the CCPA model, under which mandatory formal audits are reserved for high-risk data processing activities.

3.Third, the establishment of a U.S.–Nigeria Digital Trade Working Group should be pursued as a vehicle for achieving mutual recognition of cybersecurity standards. Given that NIST CSF 2.0 is voluntarily adopted by approximately 68 percent of U.S. organizations and functions as an informal international benchmark, Nigeria's Standards Organization could formally recognize NIST-aligned frameworks as satisfying Nigerian requirements for cross-border data handling. This would reduce duplicative compliance obligations for platforms such as Flutterwave and Interswitch operating across both jurisdictions.

4.Fourth, digital tax coordination warrants attention. Nigeria's 7.5 percent VAT on digital services should be waived for Nigerian firms utilizing U.S.

infrastructure where annual expenditure does not exceed \$500,000, thereby preventing double taxation on firms already subject to U.S. obligations. The United States has formally characterized Nigeria's digital services tax-adjacent measures as trade barriers; calibrated exemptions would preserve revenue flows for Nigeria while substantially reducing bilateral friction.

Taken together, these measures would materially improve investor confidence and accelerate Nigeria's integration into global digital supply chains.

Conclusion

This article has demonstrated that regulatory misalignment between Nigeria and the United States imposes measurable and avoidable costs on fintech firms, e-commerce platforms, and creative industries. The structural barriers identified, divergent data transfer regimes, incompatible cybersecurity standards, asymmetric compliance burdens, and uncoordinated digital taxation, are not inherent features of the bilateral relationship but remediable policy gaps. Aligning cross-border data transfer rules, adopting tiered audit thresholds, achieving mutual recognition of cybersecurity standards, and coordinating digital tax policy would, in combination, substantially reduce regulatory friction and enhance the conditions for U.S. capital deployment in Nigeria's digital economy.

Nigeria's ongoing consolidation of its data protection architecture, under the Nigeria Data Protection Act and GAID 2025, presents a strategic opportunity to embed harmonization principles at the formative stage of the regulatory framework. The measures proposed in this article, adequacy determinations, tiered compliance thresholds, cybersecurity mutual recognition, and targeted tax coordination, are consistent with the broader comparative regulatory literature on reducing friction in asymmetric bilateral trade relationships while preserving developmental policy space. Translating these recommendations into practice will require sustained engagement from policymakers, regulators, and industry stakeholders in both countries. The governance choices made in this period will shape the long-term trajectory of U.S.–

Nigeria digital trade relations and determine whether Nigeria can realize its potential as a leading hub in the global digital economy.

References

- IMARC Group, “Nigeria Fintech Market Size, Share, Trends & Forecast 2033” (Market report, 2023), available at: <https://www.imarcgroup.com/nigeria-fintech-market> (accessed 29 November 2025).
- Mordor Intelligence Source, “E-commerce is expected to hit \$16.83 billion by 2030”, available at: <https://www.mordorintelligence.com/industry-reports/b2c-ecommerce-market> (accessed 29 November 2025)
- Peterson Institute for International Economics, “The Future of the USMCA” (Web article, 2025), available at: <https://www.piie.com/microsites/2025/future-usmca> (accessed 29 November 2025).
- Ernst & Young, “US initiates review of other countries’ imposition of digital services taxes on US companies and opens comment period on nonreciprocal trade arrangements” (Tax News Update, 21 February 2025), available at: <https://taxnews.ey.com/news/2025-0549-us-initiates-review-of-other-countries-imposition-of-digital-services-taxes-on-us-companies-and-opens-comment-period-on-nonreciprocal-trade-arrangements> (accessed 29 November 2025).
- California Privacy Protection Agency, “CPPA adopts regulations on automated decision-making technology, effective January 1, 2026” (Regulatory announcement, 23 September 2025), available at: <https://cppa.ca.gov/announcements/2025/20250923.html> (accessed 29 November 2025).
- Balbix, “NIST Cybersecurity Framework 2.0: What’s New and Why It Matters” (Web article, 2024), available at:

<https://www.balbix.com/insights/nist-cybersecurity-framework/> (accessed 29 November 2025).

- Cybersecurity Tribe, “NIST ranked 2025’s most valuable cybersecurity framework” (Web article, 2025), available at: <https://www.cybersecuritytribe.com/articles/nist-ranked-2025s-most-valuable-cybersecurity-framework> (accessed 29 November 2025).
- Aluko & Oyebode, “Introducing the Nigeria Data Protection Act 2023 (NDPA)” (Client briefing, June 2023), available at: <https://www.aluko-oyebode.com/insights/nigeria-data-protection-act-2023-ndpa/> (accessed 29 November 2025).
- Banwo & Ighodalo, “Are You GAID 2025 Ready? Navigating Nigeria’s GAID 2025 – What Your Organisation Needs to Know” (Client alert, 10 August 2025), available at: <https://www.banwo-ighodalo.com/grey-matter/are-you-gaid-2025-ready-navigating-nigerias-gaid-2025-what-your-organisation-needs-to-know-how-bi-can-support-your-compliance-journey/> (accessed 29 November 2025).
- Aluko & Oyebode, “General Application and Implementation Directive (GAID) 2025” (Client update, 2025), available at: <https://www.aluko-oyebode.com/insights/general-application-and-implementation-directive/> (accessed 29 November 2025).
- Aluko & Oyebode, “NDPC Data Protection Compliance 2025: NDPC Lists 1,368 Organizations” (Client alert, 2025), available at: <https://www.aluko-oyebode.com/insights/ndpc-data-protection-compliance-2025/> (accessed 29 November 2025).
- LegalDigital NG, “Cybersecurity Laws in Nigeria: A Comprehensive Guide for Businesses Going Digital in 2025” (Practice guide, 2025), available at: <https://legaldigitalng.com/cybersecurity-laws-in-nigeria-a-comprehensive-guide-for-businesses-going-digital-in-2025/> (accessed 29 November 2025).

- Extensia, “Nigeria prepares cybersecurity regulatory framework for telecoms sector” (News article, 2025), available at: <https://extensia.tech/nigeria-prepares-cybersecurity-regulatory-framework-for-telecoms-sector/> (accessed 29 November 2025).
- Brandicon Image, “OpenAI to begin charging VAT on ChatGPT subscriptions in Nigeria” (News article, 20 October 2025), available at: <https://www.brandiconimage.com/2025/10/openai-to-begin-charging-vat-on-chatgpt.html> (accessed 29 November 2025).
- VATCalc, “Nigeria: VAT on goods and digital services for non-residents (7.5% rate, Jan 2021)” (Country summary, 2025), available at: <https://www.vatcalc.com/nigeria/nigeria-vat-on-goods-digital-services-jan-2021-for-non-residents/> (accessed 29 November 2025).
- Wyze, “Navigating Fintech in Nigeria: Balancing Growth, Regulation and Innovation” (Insight article, 17 May 2025), available at: <https://wyze-ng.com/navigating-fintech-in-nigeria-balancing-growth-regulation-and-innovation/> (accessed 29 November 2025).
- Duplo, “Cross-Border Payments in Africa: Challenges, Opportunities and How Duplo Fits In” (Blog article, 29 September 2025), available at: <https://tryduplo.com/blog/cross-border-payments-in-africa-challenges-opportunities-and-how-duplo-fits-in/> (accessed 29 November 2025).
- Olaniwun Ajayi LP, “Creative Wrap-Up Report and Outlook 2025” (Industry report, 3 February 2025), available at: <https://www.olaniwunajayi.net/blog/creative-wrap-up-report-and-outlook-2025/> (accessed 29 November 2025).

End Page

Thank you for reading the Journal of IP Professionals (JIPPS)

The Digital Economy and the Law: Intellectual Property, Technology, and Global Trade.

Volume 2 (2026)

For inquiries, submissions, or permissions, please contact us at:

Email: hellojipps@zohomail.com

Website: <https://jipps.letstalkipwithdaphne.org/>

Follow us for updates and future calls for papers.

"Creativity is the currency of the future, and intellectual property is its protector."

© 2026 Journal of IP Professionals (JIPPS). All rights reserved.

All articles remain the intellectual property of their respective authors. No part of this journal may be copied or reused without appropriate authorization.