

Chapter 13

Beyond Firewalls: Copyright, AI Content, and the Cybersecurity Reality Check

Abu Zar, Assistant Professor, School of Legal Studies, Swami Vivekananda University

Abstract

Cybersecurity has historically been viewed as being a technical-based discipline such as firewalls, encryption and intrusion-detection systems²⁴⁵. With the rapid adoption and spread of artificial intelligence (AI) in the creation of content, we have now entered a new phase of Digital Security, which combines copyright law with Intellectual Property Rights (IPR) at the intersection of AI-generated content with cyber security²⁴⁶. This chapter will show how the commonly-held view that cyber security is a solely technical discipline has blinded us to the fact that legal loopholes — many of which stem from AI-generated content — can represent significant threats to cybersecurity as well.

The introduction of generative AI has introduced disruptions to existing copyright systems, which have traditionally been structured around human authorship²⁴⁷. As a result, many questions remain about originality, ownership and liability for works created by AI, meaning that they exist in a legal grey area. Courts and legislators across the globe have struggled to apply established concepts of copyright law in the context of machine-generated creations, such as whether works generated by machines can be protected under copyright law and whether existing copyright holders have been infringed by the use of their protected materials to train the AI systems that produce these works²⁴⁸. These issues have major relevance to the cyber security space since malicious actors are using ambiguities in copyright as a means of perpetrating takedown abuse, spreading of misinformation and perpetrating data poisoning attacks through the weaponization of intellectual property disputes in cyberspace.

This chapter situates the issues discussed herein against the greater Cybersecurity Myth-Reality Divide. It will examine where copyright disputes interact with threats emanating from the cyber domain, showing how the lack of a clear legal framework erodes confidence in the digital ecosystem. It does so by relying on several increasingly prominent scholarly articles related to these matters, such as Jiang et al.'s Blockchain Enabled Approaches to AI Copyright Management²⁴⁹; Yang & Zhang's Economic Modelling of Fair Use and AI Copyrightability²⁵⁰; and Muthu's analysis of current Indian and International Copyright Law²⁵¹. As such, all sides will have access to both the global and jurisdictionally specific aspects of the challenge at hand.

²⁴⁵ Christopher T Zirpoli, *Generative Artificial Intelligence and Copyright Law* (CRS, 2025).

²⁴⁶ Astha Ojha, *AI & Copyright in India: Law, Policy, and the Future of Creative Rights* (MeitY, 2024).

²⁴⁷ Asmi Vikas Kedare, 'The Impact of Generative AI on Copyright Law in India' (SSRN, 2024).

²⁴⁸ *ibid.*

²⁴⁹ Jiang et al, 'Blockchain Enabled Approaches to AI Copyright Management' (2023) *JIPTL* 45.

²⁵⁰ Yang & Zhang, 'Economic Modelling of Fair Use and AI Copyrightability' (2022) *IRLE* 71.

²⁵¹ Muthu, 'Analysis of Current Indian and International Copyright Law in the Age of AI' (2023) *IJLT* 19(2).

The chapter will also argue that to achieve strong cybersecurity, it will be necessary to build upon both technical defences as well as strong legal and/or policy frameworks to meet the real-life challenges submitted by AI to traditional perceptions regarding copyright ownership.

Ultimately, the chapter will call for hybrid solutions that bring together law, technology and policy. By bridging the gap between the legitimate and illegitimate perceptions of ownership and the actualities created by AI-based content creation, the chapter aims to develop a blueprint for how to secure digital creativity in a world dominated by generative AI²⁵². The chapter will also assist in furthering the overall realm of *Beyond Firewalls* which highlights how to build a successful cybersecurity infrastructure through the recognition and mitigation of the inherent legal risks associated with digital innovation.

Keywords: *International Copyright Law, Firewalls, Encryption And Intrusion-Detection Systems.*

Introduction: Cybersecurity Beyond the Technical Lens

Traditionally, cybersecurity is seen as a strictly technical field comprised of firewalls, encryption methods, and intrusion detection systems²⁵³. Nevertheless, that viewpoint only tells a piece of the story; in reality, cybersecurity has many legal, social, and ethical issues associated with it – especially now that we are living in an era where AI is changing what we understand as creative works²⁵⁴. As automated creativity continues to produce new forms of text, images, music, and code, the scope of traditional intellectual property law will be pushed to its limits. Therefore, it is a myth that cybersecurity can be achieved through technical means alone because, at the same time, new questions regarding the authorship, ownership, and liability of AI-generated content create additional vulnerabilities and risk of exploitation²⁵⁵.

Thus, many aspects of copyright law which were developed with the evaluation of human creativity have now been disrupted by the increasing prevalence of generative AI. Historically, copyright law has assumed that a human author creates a work using their skills, judgement, and originality to produce an expression that is eligible for copyright protection. Conversely, it is now possible for an AI system trained on millions of sets of data to generate outcomes that are like human creativity though there was not an actual human author involved in producing the outputs in question. Consequently, two important issues arise: (1) whether AI-generated works are eligible for copyright protection; and (2) who should receive credit as the author of an AI-generated work? Answering these questions are important from the perspective of cybersecurity because unresolved issues of ownership provide significant opportunities to exploit others²⁵⁶.

²⁵² Zirpoli (n 2).

²⁵³ Zirpoli (n 2).

²⁵⁴ Ojha (n 3).

²⁵⁵ Kedare (n 4).

²⁵⁶ *ibid.*

Adversaries can exploit copyright-based claims to impede operations across digital platforms by filing false claims or issuing bogus takedown notices, thus allowing them to disrupt digital platforms, disseminate misinformation, or damage confidence levels among the members of online systems at scale²⁵⁷. Because of these dynamics, the difference between the myth and reality is much more pronounced than typical cases of disagreement between claims of property rights and the real rights attached to an object.

The myth is that generative (AI produced) media is completely “free” or “ownerless,” thus creating an argument that it can be used by anyone without restrictions. In contrast, the reality is that while generative content may exist, it exists in an area where the ability to determine who is liable or entitled to use generative content is constantly shifting due to competing claims of ownership or use of that material²⁵⁸. As generative technologies create new types of vulnerabilities and introduce new issues related to cybersecurity, it is necessary to protect and privilege existing intellectual property laws as part of the underlying protection of any content available to the public.

A growing body of literature has begun creating avenues for addressing these issues through the application of existing, recent works. Jiang et al. offer blockchain based frameworks for managing generative media leveraging concepts related to maintaining trust-based lifecycle records and executing trusted, independent third-party audits throughout the entire life of the media²⁵⁹.

In their article, Yang and Zhang look at how both copyright law and fair use impact the economics of generative AI²⁶⁰. They discuss the ongoing conflict between promoting innovation and regulating it. Muthu analyses both Indian and international copyrights and examines how each jurisdiction has a different set of challenges to incorporating AI into their respective statutory frameworks²⁶¹. The combination of these two studies demonstrates that the notion that AI-generated creativity is clear and defined ownership has failed; AI creativity exists in a fragmented and contentious environment and is inherently tied to cybersecurity issues.

This chapter examines this debate in relation to the wider context of the 'myth-reality divide' in cybersecurity. The chapter develops the argument that that effective cybersecurity requires not only technical defences but also legal and policy structures that can adapt to deal with the realities of AI-generated creativity²⁶². It uses a framework examining the relationship between copyright law, AI content, and cybersecurity to illuminate the myths that prevent the understanding of these vulnerabilities and to highlight the realities that must be addressed. Therefore, it supports a broader understanding of cybersecurity as a whole—an understanding that incorporates both technical and legal factors to provide security to digital creativity.

²⁵⁷ Zirpoli (n 2).

²⁵⁸ Muthu (n 8).

²⁵⁹ Jiang et al (n 6).

²⁶⁰ Yang & Zhang (n 7).

²⁶¹ Muthu (n 8).

²⁶² Ojha (n 3).

The Myth of AI Creativity and Ownership

There are many myths surrounding artificial intelligence and one of them is that AI-generated works are neutral (i.e., unbiased), free (i.e., chargeable to no person), and unowned (i.e., unowned by anyone)²⁶³. Part of this myth stems from a belief that machines cannot create nor claim authorship as they don't possess the same capacity to create because they're machines. However, the truth is much more complicated. Generative AI is trained on huge amounts of data and produces works with some quality of originality and artistic merit. Thus these "neutral" speaking outputs exist in a contested legal and moral environment²⁶⁴.

Copyright has been historically defined based on human authorship. Under the Berne Convention, copyright assumes creative works will come from identifiable people who can exert intellectual effort into creating the output²⁶⁵. Additionally, The TRIPS Agreement also places copyright within trade and enforceable structures and promotes a human-centred approach²⁶⁶. Therefore, generative AI disrupts this basis of all established rules of copyright law as they produce works without any direct involvement by humans. Thus, courts and lawmakers have had difficulty deciding whether to protect generative AI works under existing copyright law. For example, the US Copyright Office has explicitly ruled that works solely created by a generative AI are not entitled to copyright protection²⁶⁷, thus further entrenching the belief that the output of a generative AI has no legal significance.

The "Myth of the Free Content" is another example of how AI's creative capacities are ignored, including the economic and ethical implications associated with the use of creativity created by Artificial Intelligence (AI)²⁶⁸. AI's reliance on datasets to develop and produce creative work often has significant implications for copyright law and the concept of fair use, as training data sets frequently include works subject to copyright protection. Because many AI-based systems use creative work protected by copyright law to generate their output, the resulting creative work should not be regarded as neutral and free from any legal obligations. As a result, both users and developers of AI-generated creative works risk being held liable, which undermines the perception that AI creativity exists outside of the sphere of protection offered under Intellectual Property law²⁶⁹.

Scholars have expressed concern that allowing this myth to persist creates risk for the future of creative industries. For example, Andres Guadamuz posits that by removing AI-generated works from copyright protection, the creative economy would be negatively impacted because unlimited exploitation of original creative works would occur without compensating the original creator²⁷⁰. Similarly, Pamela Samuelson stresses that copyright law must adapt to the digital world in which we live, including the unique way Artificial Intelligence produces creative works, to preserve copyright's

²⁶³ Zirpoli (n 2).

²⁶⁴ Kedare (n 4).

²⁶⁵ Berne Convention for the Protection of Literary and Artistic Works (Paris Act 1971).

²⁶⁶ Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS, 1994).

²⁶⁷ US Copyright Office, *Copyright Registration Guidance: Works Containing AI-Generated Material* (2023).

²⁶⁸ Samuelson (n 28).

²⁶⁹ Yang & Zhang (n 7).

²⁷⁰ Andres Guadamuz, 'Artificial Intelligence and Copyright' (2017) WIPO Magazine.

legitimacy²⁷¹. Yang and Zhang provide an economic analysis of the relationship between Copyright and Fair Use by providing a mathematical model demonstrating how allowing unlimited use of generative AI-created works would eliminate incentives to innovate in the creative community²⁷². Finally, Muthu's analysis of the law in India emphasises that the lack of clear, enforceable rules in relation to AI-generated creative works creates uncertainty in cyberspace, which can result in the exploitation of those works by individuals and/or entities that reside outside of the jurisdiction of the creator²⁷³.

Thus, it follows that AI Creative must be viewed in the larger picture of the ecosystem around it which includes the rights, obligations and exposure of this ecosystem to security risk²⁷⁴. As ownership, liability and ethical issues are inseparable from the risk of Generative AI technology publicly exposing the myth of neutrality while exposing the reality of contestable nature of AI Creative, this chapter highlights the fact that the complexities of machine-generated content must be recognised and reflected in legal constructs.

Copyright in the Age of Generative Algorithms

The rise of generative algorithms has had significant effects on copyright law²⁷⁵. Copyright laws were originally created for human creators and are based on the idea that creative works are the outcome of the expertise of an individual. When it comes to generative AI, though, the output is created without much involvement from the artist or human creator. Because there is no human author creating an art piece, it is not clear whether it meets the requirements of copyright law with respect to originality and authorship²⁷⁶.

International treaties such as the Berne Convention and TRIPS Agreement do not address this issue, meaning that they support copyright based on human authors²⁷⁷. In practice, different countries have responded differently to this problem; for example, the US Copyright Office has decided that they will not protect works that were created by AI alone²⁷⁸, while the UK Intellectual Property Office has allowed for limited recognition of works created with assistance from AI²⁷⁹.

Copyright has become highly debated when it comes to AI-created works, especially with respect to originality. Courts have required “a minimal amount of creativity” or “a substantial degree of intellectual effort” for the establishment of copyright²⁸⁰, and the originality of an AI-produced work is less certain than a traditional creative work because AI-generated works lack human intention. Guadamuz and others have pointed out that excluding AI works entirely might undermine the creative

²⁷¹ Pamela Samuelson, ‘Copyright Law and the Digital Age’ (2019) *Journal of Intellectual Property Law*.

²⁷² Yang & Zhang (n 7).

²⁷³ Muthu (n 8).

²⁷⁴ Muthu (n 8).

²⁷⁵ Zirpoli (n 2).

²⁷⁶ Kedare (n 4).

²⁷⁷ Berne Convention (n 22), TRIPS Agreement (n 23).

²⁷⁸ US Copyright Office (n 24).

²⁷⁹ UK Intellectual Property Office, *Consultation on Artificial Intelligence and Copyright* (2021).

²⁸⁰ US Supreme Court, *Feist Publications v Rural Telephone Service Co* 499 US 340 (1991).

industry²⁸¹, while authors such as Weatherall caution that including AI works might dilute the concept of authorship²⁸².

With respect to liability, there is great uncertainty about who would be liable if an AI-created work is infringing: the developer of the AI, the user or any of the prior datasets²⁸³. This uncertainty has ramifications for cybersecurity—as malicious actors can exploit the lack of clarity in liability rules to publish infringing or harmful materials and give little (or no) attribution/accountability to any party.

Recent approaches have suggested hybrid solutions. Giblin and Weatherall have stressed the importance of ensuring that any dataset used to train an AI meets copyright obligations through using a transparent dataset²⁸⁴. Jiang et al are proposing blockchain-based systems to provide for accountability and tracing back through the lifecycle, allowing an AI-generated work to be traced back to its source(s)²⁸⁵. These types of approaches support the conclusion that to adequately protect AI-generated works, legal protections need to be in place which incorporate technological safeguards.

In summary, copyright for AI-generated works is currently fragmented and contested, but large developments are likely to occur soon²⁸⁶. The perception that ownership can be clearly defined has been replaced by an understanding that there is a considerable amount of uncertainty over various aspects of cyberspace. Laws and treaties at both the nation-state and international level, as well as substantial academic discourse surrounding the subject, have not kept up with the rapidly evolving landscape of technology. Beyond being a legal issue, uncertainty creates risks associated with the security of digital ecosystems, resulting in a loss of confidence in cyberspace and exposing opportunity for exploitation²⁸⁷.

Intersecting Domains: Copyright Disputes as Cybersecurity Risks

Digital vulnerabilities resulting from the intersection between copyright law and cybersecurity are one of the most critical yet underappreciated areas of research²⁸⁸. Historically, copyright issues revolved around ownership and infringement, but copyright is now used as a source of cyber conflict with both malicious uses of copyright law and intellectual property as a means of disrupting digital platforms through the weaponization of takedown notices, automatic content filter systems, and threats of lawsuits²⁸⁹.

One illustration of how copyright is exploited as a source of cyber disruption is through the misuse of the Digital Millennium Copyright Act (DMCA) takedown provision²⁹⁰. The DMCA was designed to

²⁸¹ Andres Guadamuz, 'Artificial Intelligence and Copyright' (2017) WIPO Magazine.

²⁸² Kimberlee Weatherall, 'AI and the Concept of Authorship' (2020) *UNSW Law Journal*.

²⁸³ Samuelson (n 28).

²⁸⁴ Rebecca Giblin and Kimberlee Weatherall, 'AI Training Data and Copyright Transparency' (2022) *Journal of Intellectual Property Law & Practice*.

²⁸⁵ Jiang et al (n 6).

²⁸⁶ Muthu (n 8).

²⁸⁷ Yang & Zhang (n 7).

²⁸⁸ Zirpoli (n 2).

²⁸⁹ Kedare (n 4).

²⁹⁰ Digital Millennium Copyright Act 1998 (US).

protect the rights of copyright owners but has been misused to silence competitors, promote misinformation, or otherwise disable legitimate content. Viewed through the cybersecurity lens, this represents a legal denial of service attack against online systems and thus erodes confidence in the online economy.

The proliferation of generative AI technologies complicates this issue. For example, deepfakes and synthetic media created by training on copyrighted materials result in a grey area that blurs between legal infringement and manipulation²⁹¹. Where copyright disputes involve disinformation campaigns, the confluence of copyright and cyber threats creates a hybrid threat with both legal uncertainty and technical exploitation. This convergence of copyright and cybersecurity shows that copyright is no longer at the periphery of cybersecurity but is crucial to its integrity.

The response to policies is inconsistent and lacking. While the EU Digital Services Act sets an obligation on platforms to tackle illegal activity online, i.e., copyright issues, etc., it does not have fully developed methods for enforcing it yet²⁹². In addition, as Bruce Schneier points out, there are equally as many risks when it comes to the law itself containing legal vulnerabilities as there are with technology - adversaries will exploit whichever vulnerability offers them the greatest access²⁹³.

Copyright disputes now operate as vectors for creating cyber insecurity; therefore, if policymakers and scholars can identify this intersection, they could take steps to end the myth that intellectual property laws are in some way different than those governing cyber security²⁹⁴. Owners of intellectual property rights and the material they own are continuously in conflict; there are gaps in liability coverage; and enforcement mechanisms are needed to provide the stability needed in digital networks.

Case Studies: Law, AI, and Digital Vulnerabilities

Copyright disputes intersect with cybersecurity risks in practice, and case studies provide concrete examples of the way these two areas intersect. Generative AI presents challenges that are not just theoretical--but rather are posed by real legal conflicts and risks posed by technologies used to create generative AI²⁹⁵.

A notable example is the case concerning AI-generated art platforms. A group of artists filed suit against Stability AI based on allegations of infringement of their works by Stability AI's training datasets (2023)²⁹⁶. This case illustrates how unresolved questions concerning the legality of the datasets used for training generative AI can lead to a large-scale dispute and cybersecurity risks. If the training data is unlawfully obtained or manipulated, the resulting generative AI images can create both legal

²⁹¹ Samuelson (n 28).

²⁹² Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act).

²⁹³ Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (WW Norton 2018).

²⁹⁴ Muthu (n 8).

²⁹⁵ Zirpoli (n 2).

²⁹⁶ *Andersen et al v Stability AI Inc* (US District Court, ND Cal, filed 2023).

liability and reputation damage for the platform(s) that use the training data to create generative AI images.

Another example of legal jeopardy related to generative AI and cybersecurity is the use of deepfake technology in political campaigning. Courts and regulators regularly wrestle with legal issues concerning whether deepfakes are a form of copyright infringement, defamation, or a threat to the cybersecurity of political campaigns²⁹⁷. The difficulty with applying established legal categories to AI outputs is illustrated by the hybrid nature of deepfakes (creative, deceptive, or potentially infringing), which makes it difficult for courts to determine the applicability of traditional legal categories.

Additionally, in India, the issue of copyright in respect of AI-generated educational material has raised jurisdiction-specific issues related to cybersecurity²⁹⁸. Institutions lack necessary statutory guidance to make determinations as to whether AI-generated materials may be owned, licensed, or protected. Because there is no certainty about how to handle copyright violations across different jurisdictions (countries) and continents (areas), this creates the possibility that bad people will capitalize on the gap left by enforcement (those "bad actors") and destroy trust in digital learning systems (the Internet).

The case study presented in this chapter support a larger theme within this chapter: that copyright issues are not just an isolated legal problem, but also a cybersecurity issue²⁹⁹. They also show how ownership issues, lack of liability, and lack of an effective (or even appropriate) means of enforcing copyright protection can lead to a breakdown in the digital world and illustrate that technical cybersecurity by itself does not exist.

Global Legal and Policy Perspectives

Artificial intelligence governance and the intersections of copyright and data security law are widely disparate³⁰⁰. Instead of a coherent international standard, we see a collection of divergent nations' laws, regional regulations, consultation forums, and other policies. The diverse landscape is more than a technical challenge—it is a dereliction of the fundamental infrastructures. Because rules differ across borders, nations, regions, and continents create avenues for individuals to use technological loopholes to exploit weaknesses in copyright enforcement and undermine the resilience of organizations to respond to cybersecurity vulnerabilities³⁰¹.

European Union: A Holistic Approach

AI regulation in Europe is leading the world. The AI Act creates a risk-based classification system for AI systems that sets strict requirements for transparency, accountability, and documentation of datasets from high-risk AI system providers³⁰². Although the AI Act is not a copyright law, it indirectly

²⁹⁷ Chesney and Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.

²⁹⁸ Muthu (n 8).

²⁹⁹ Kedare (n 4).

³⁰⁰ Zirpoli (n 2).

³⁰¹ Kedare (n 4).

³⁰² Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM (2021) 206 final.

influences the debates about who owns the copyright by establishing a requirement for provenance records for training data. This means that the use of datasets that include protected works is problematic in the copyright context for most generative models. The European Union expects that by creating a mandatory disclosure requirement, it can reduce infringement risk and increase cybersecurity through traceability.

The **Digital Services Act (DSA)** helps create an EU-wide regulatory framework by requiring platforms to remove all illegal content from their services, including content that infringes on copyrights, within a specified time frame³⁰³. The AI Act and DSA work collaboratively as part of an overall regulatory approach where copyright enforcement is a component of the larger digital governance process and is inextricably linked to cybersecurity. The EU is positioned as a normative leader in this area and seeks to export its regulatory regime globally through trade agreements and digital partnerships³⁰⁴.

United States: Fragmentation and Litigation

In comparison to how it has responded, the United States government is fragmented and typically responds reactively. The Copyright Office has issued clarifying opinions that deny copyright to anything made by only an artificial intelligence, thereby upholding a fundamentally human-based model of authorship. But there are no federal statutes yet regulating the use (and/or creation) of artificial intelligence³⁰⁵. Rather, private parties are responsible for mostly enforcing the current copyright laws through traditional litigation as well as by acting under the **Digital Millennium Copyright Act ("DMCA")**³⁰⁶. Additionally, the current DMCA system has been used by malicious actors to attack others. Copyright claims are often used strategically by competitors (i.e., the person asserting copyright over a protected work and/or the company asserting copyright over the work) to disrupt the ability of legitimate parties to provide their product/content to the market or to disrupt their ability to use a particular platform — in essence, to create a denial of service through lawful processes³⁰⁷.

This reliance on a litigation-based system creates uncertainty about cybersecurity (which has also increased in recent years). In this sense, the copyright system and the cybersecurity system remain separate; however, they are becoming increasingly dependent on one another. The US approach is consistent with a market-driven philosophy of governance, but it is riddled with many substantial gaps that adversarial parties can take advantage of.

³⁰² Digital Services Act (n 49).

³⁰³ *ibid*

³⁰⁴ US Copyright Office (n 24).

³⁰⁵ DMCA (n 47).

³⁰⁶ Samuelson (n 28).

³⁰⁷ Guadamuz (n 27).

Asia: Hybrid Models and Cautious Approaches

There are varied approaches taken by Asian countries about this area. For example, China has issued regulations governing deep synthesis technologies, which require those who operate or create synthetic content to identify themselves, as well as preventing the misuse of synthetic content³⁰⁸. These obligations link the enforcement of copyright with cybersecurity and recognize that the production and distribution of synthetic media have both legal implications and security risks. By having these requirements in place, China hopes to limit disinformation campaigns and protect the rights of content creators.

India has not legislated on the issue of creativity produced through AI technologies to date; however, Indian courts and scholars have made it clear that human authorship is the fundamental basis for copyright protection and have taken a conservative approach to extending the protection of copyright to works created by machines³⁰⁹. This conservative approach avoids giving legal recognition to the authorship of AI-generated works currently, but results in limited enforcement mechanisms against those who engage in producing and distributing such works. Practically speaking, this uncertainty creates significant exposure to risks for organizations, platforms, and other stakeholders who are susceptible to being exploited by individuals using malicious tactics that benefit from existing regulatory uncertainty.

International Organisations: The Struggle for Harmonisation

The World Intellectual Property Organization (WIPO) has started an initiative on the relationship between artificial intelligence and intellectual property law on an international level, with the goal of garnering input on this topic³¹⁰. The urgency of harmonizing international intellectual property laws has become apparent because of the international nature of disputes regarding the creation of works by artificial intelligence. However, few countries have come to agreement about how laws will be harmonized, and developed countries tend to advocate for the incentive to develop innovation; developing countries are more apt to support equitable access and protection from the exploitation of creative works³¹¹.

The lack of agreement on how the use of artificial intelligence should be regulated has led to the escalation of copyright disputes regarding works created by artificial intelligence being thrown into questions of jurisdiction³¹². An example of this would be when local law adheres to the local exception for copyright protection and the creation of the work is illegal outside of that country. The lack of international cognition regarding copyright dispute resolution leads to a set of issues related to trust in the digital ecosystem as well as systemic vulnerabilities.

³⁰⁸ Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis Internet Information Services* (2022).

³⁰⁹ Muthu (n 8).

³¹⁰ World Intellectual Property Organization (WIPO), *WIPO Conversation on Intellectual Property and Artificial Intelligence* (2020).

³¹¹ *ibid.*

³¹² Yang & Zhang (n 7).

Towards Convergence

There is evidence that there are some trends moving parties toward a convergence of opinions and laws regarding artificial intelligence, including an increasing emphasis on transparency in relation to the training dataset, accountability for outputs and liability of parties for the misuse of training datasets and/or the outputs created from them³¹³. These principles suggest an acceptance that there are interdependencies between copyright and the cybersecurity community relative to their respective roles in developing a governance system for digital commerce. Moving forward, the challenge will be to create enforceable international covenants between all parties regarding these principles³¹⁴.

Bridging the Divide: Towards Hybrid Legal–Technical Solutions

Due to the ongoing global fragmentation of copyright laws and the rapid advancement of generative artificial intelligence (AI) technologies, there is an urgent need for hybrid solutions that bring together legal and technological measures³¹⁵. While both laws and technologies can assist in addressing the challenges posed by AI generated materials individually, it is the shared responsibility of each discipline to effectively address these challenges. Addressing the legal challenges presented by AI consists of providing a comprehensive strategy that incorporates norm-based regulation along with technical measures. There are copyright litigation challenges; liability gaps for products used by AI; and cybersecurity risks associated with AI that require coordinated solutions combining traditional regulatory mechanisms with innovative technological solutions.

The Limits of Purely Legal Responses

Generative algorithms are too complex for traditional copyright law³¹⁶. The requirement for human authorship remains theoretically sound, the real-world problem lies in the non-human nature of autonomous creativity via machines. The judicial and legislative branches of government have had difficulty identifying how to respond too many courts and legislatures have resorted to narrowly interpreting traditional copyright laws thus denying copyright protection for certain passive forms of AI outputs. This provides protection of the integrity of an authorship; however, passive forms of AI outputs circulate within the marketplace without clear affiliation to any party which creates ambiguity amongst creators, platforms and users.

In addition, enforcement methods that are based solely on legal remedies have been shown to be ineffective, particularly in a cyberspace context, where they tend to fall within the reactive category of remedy, rather than the proactive category of remedy. As a result, once a court or other legal body has concluded that there is an infringement, it does not cure the harm or resolve the underlying issues because of the inherent delay in investigations and resolution processes³¹⁷ unique to cyberspace, and

³¹³ Giblin and Weatherall (n 41).

³¹⁴ *ibid.*

³¹⁵ Zirpoli (n 2).

³¹⁶ US Copyright Office (n 24).

³¹⁷ Samuelson (n 28).

as a result, malicious actors exploit this ambiguity to disseminate infringing or harmful content without consequence.

Generative algorithms are too complex for traditional copyright law. The requirement for human authorship remains theoretically sound, the real-world problem lies in the non-human nature of autonomous creativity via machines. The judicial and legislative branches of government have had difficulty identifying how to respond too many courts and legislatures have resorted to narrowly interpreting traditional copyright laws thus denying copyright protection for certain passive forms of AI outputs. This provides protection of the integrity of an authorship; however, passive forms of AI outputs circulate within the marketplace without clear affiliation to any party which creates ambiguity amongst creators, platforms and users.

In addition, enforcement methods that are based solely on legal remedies have been shown to be ineffective, particularly in a cyberspace context, where they tend to fall within the reactive category of remedy, rather than the proactive category of remedy. As a result, once a court or other legal body has concluded that there is an infringement, it does not cure the harm or resolve the underlying issues because of the inherent delay in investigations and resolution processes unique to cyberspace, and as a result, malicious actors exploit this ambiguity to disseminate infringing or harmful content without consequence.

The Limits of Purely Technical Responses

Technical safeguards like watermarking, dataset transparency and blockchain based provenance offer new possibilities for managing AI output. Jiang et al suggest using blockchain technology to create a lifecycle record that will allow for traceability³¹⁸ of AI generated works. Watermark technologies can embed identifying information within synthetic media, allowing for the identification and prevention of misuse of those media.

However, technical solutions alone cannot answer normative questions regarding ownership, liability, and authorship³¹⁹. While watermarks may provide evidence of provenance, they do not determine copyright status. Although blockchains will provide a record of the lifecycle of a work, they cannot resolve disputes regarding fair use or infringement. Without legal recognition, these technical safeguards may go unused or be ignored.

Towards Hybrid Governance

Hybrid governance models look to merge the legal and technological ways to govern through copyright and cybersecurity, given the interconnectedness of the two areas, and necessitating a collaborative approach to ensuring adequate regulation on both fronts.

An approach of how this is occurring is through embedding legal duties into technical architecture³²⁰, such as when the EU's AI Act imposes requirements for transparency regarding training datasets; this

³¹⁸ Giblin and Weatherall (n 41).

³¹⁹ EU AI Act (n 49);

³²⁰ Digital Services Act (n 49).

legal obligation can be fulfilled using technical solutions like dataset registries or blockchain records. As a result of the integration of both legal and technical solutions, compliance with these legal duties would not only be a matter of being declared but also providing verifiable technology for compliance.

Another approach of how interconnectedness between copyright and cybersecurity will provide an improved governance model is through establishing liability frameworks that allocate responsibility across all stakeholders; developers, platforms, and users should share some amount of responsibility for the output of AI technologies and use technical safeguards as evidence of legal accountability. For instance, if a platform incorporates watermarking to identify synthetic media that is deployed on a platform, but the platform does not act when that synthetic media is identified, the platform may be liable based on its failure to meet its obligation to act against illegal activity. By providing an incentive for legal compliance as well as for due diligence with respect to compliance, the hybrid approach will advance governance models for both copyright and cybersecurity.

Ethical and Policy Dimensions

There are ethical considerations that must be addressed in hybrid solutions. There is a moral obligation as well as a legal one to make datasets transparent to honour the rights of the creator in the dataset. There are also technical issues associated with watermarking technologies. These watermarking technologies must balance privacy with detection. Watermark technologies must have the capability to detect a watermark without being able to reveal any confidential information about an individual. Policymakers will need to develop frameworks that provide for ethical safeguards in both law and technology. They will need to develop these frameworks with the understanding that legitimacy cannot be achieved solely through compliance. International cooperation is necessary for hybrid solutions to be successful. WIPO's consultations on AI and IP clearly demonstrate the need for cooperation and harmonization³²¹ about AI and IP. However, an agreement on how to accomplish this has yet to be reached. Hybrid solutions may be the best way to reach a compromise. Hybrid solutions will allow states to adopt flexible technical standards while still meeting the requirements established by core principles of law. For example, states could agree to minimum requirements regarding the transparency of datasets but could allow for the local enforcement of those minimums.

Case Studies in Hybrid Approaches

Case studies of recent developments in hybrid governance show promise for this type of system. The European Union has begun integrating automated detection software with legal takedown requirements under its Digital Services Act, creating a hybrid system that combines technical monitoring with legal enforcement through a technically focused system (software) and an enforcement-based system (legal action). Another example is China's use of hybrid governance through its deep synthesis regulations, which require both the labelling of synthetic media and liability on behalf of the producer for any misuse³²² (both are regulatory requirements). The examples illustrate that hybrid models are not just

³²¹ Cyberspace Administration of China (n 65), WIPO (n 67).

³²² WIPO (n 67).

theoretical concepts but are currently in use around the world; however, the extent of their implementation and the way each jurisdiction uses them varies widely across jurisdictions.

Conclusion

The emergence of generative artificial intelligence serves to elucidate how intertwined copyright and cybersecurity are as domains³²³. What began as a debate about authorship and originality is morphing into a more comprehensive understanding that ownership disputes, gaps in liability, and enforcement mechanisms are all related to the stability of digital ecosystems. While copyright law protects human creative works, it is now faced with challenging outputs of this law's basic premise; meanwhile, cybersecurity laws must consider that, in some cases, legal ambiguity can be manipulated by attackers as an exploit vector³²⁴. This chapter has illustrated that there is no unified global approach to addressing these issues: the European Union is pursuing an integral regulatory regime through proposals such as the AI and Digital Services Acts; the United States is relying on litigation and adversarial enforcement through existing legislation such as the DMCA; and China is implementing hybrid approaches that unite copyright enforcement with cybersecurity responsibilities, while India has been more cautious and has placed emphasis on human authorship, international organisations like WIPO have started the process of engaging in consultations with their member states to create some agreement; however, there is still no clear consensus on the matter³²⁵.

There are, however, some areas in which there is more convergence among countries regarding their principles of how copyright applies: transparency of training dataset, accountability for results generated from the output and how the use of those results will not be misused³²⁶. The principles reflect an increasing understanding that copyright enforcement is not just protecting the rights of the creators but also has a direct impact on cybersecurity. This means that hybrid solutions which inject legal obligations (like Copyright) into technical protections (like Digital Rights) will ensure compliance from a normative standpoint (that is, the law needs to create a normative expectation of compliance with copyright) and from a technical standpoint³²⁷ (that is, technology must incorporate and demonstrate in a verifiable manner compliance with copyright). Moreover, to achieve true accountability from AI created by humans, the myth of AI neutrality needs to be replaced with an understanding of AI accountability³²⁸. AI's creativity cannot exist without ownership and liability; rather, it will be necessary to govern AI using a framework that integrates law, technology, and ethics. This will allow for both innovations to flourish and for the resiliency of the digital ecosystem to be enhanced³²⁹.

³²³ Zirpoli (n 2).

³²⁴ Kedare (n 4).

³²⁵ EU AI Act (n 49); Digital Services Act (n 49); DMCA (n 47); Cyberspace Administration of China (n 65); Muthu (n 8); WIPO (n 67).

³²⁶ Giblin and Weatherall (n 41).

³²⁷ Yang & Zhang (n 7).

³²⁸ Samuelson (n 28).

³²⁹ Guadamuz (n 27).