WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/16/15
ORIGINAL: ENGLISH
DATE: JANUARY 12, 2024

Advisory Committee on Enforcement

Sixteenth Session
Geneva, January 31 to February 2, 2024

ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY ENFORCEMENT

Contributions prepared by Mr. Dennis Collopy, Countercheck, Universal Music Group and Mercado Libre

1. At the fifteenth session of the Advisory Committee on Enforcement (ACE), held from August 31 to September 2, 2022, the Committee agreed to consider, at its sixteenth session, among other topics, the "exchange of information on national experiences relating to institutional arrangements concerning IP enforcement policies and regimes, including mechanisms to resolve IP disputes in a balanced, holistic and effective manner". Within this framework, this document introduces the contributions three private-sector entities (Countercheck, Universal Music Group (UMG) and Mercado Libre) on their experiences with artificial intelligence (AI) and intellectual property (IP) enforcement.

2. The contribution by Mr. Dennis Collopy summarizes the research study *Artificial Intelligence and Intellectual Property Rights Enforcement*. It clarifies key definitions, explains the methodology used and provides a comprehensive overview of the study's findings. More specifically, it identifies opportunities in using AI to enforce IP rights, such as improved detection of copyright-infringing content, design recognition and faster detection of trademark misuse. Conversely, it identifies some significant challenges, such as costs, lack of transparency, data-sharing issues and ethical considerations.

3. The contribution by Countercheck discusses the use of AI in the inspection of parcels. The contribution highlights Countercheck's technology as well as the legal challenges in implementing AI, emphasizing the need for collaboration between public and private sectors to combat IP crime and improve the legal framework.

4. The contribution by UMG highlights its views on AI, focusing on the responsible use of AI amidst deep concerns about IP infringement. It delves into concerning activities, such as using AI to mimic artists and generate fraudulent tracks and the means by which AI systems are being

trained, notably the unauthorized access to copyright-protected musical works. The contribution also underlines how AI can be used by right holders in the music industry – both as a support of the creative process and as a tool to detect infringements.

5. The contribution by Mercado Libre discusses the use of AI to automatically detect and remove listings of counterfeit goods on its e-commerce marketplace. After outlining the regulatory frameworks throughout Latin America, the contribution describes the proactive efforts Mercado Libre uses with the assistance of AI to detect counterfeit goods, as well as the difficulties of such AI use.

6. The contributions are in the following order:

[Contributions follow]

Artificial Intelligence and Intellectual Property Enforcement: Overview of Challenges and Opportunities

Contribution prepared by Mr. Dennis Collopy, Senior Research Fellow, School of Creative Arts, University of Hertfordshire, Hatfield, United Kingdom[*]

ABSTRACT

This contribution summarizes the results of the research study *Artificial Intelligence and Intellectual Property Rights Enforcement*. The contribution clarifies key definitions and explains the methodology used, before reporting on the study findings. More specifically, it identifies opportunities in using artificial intelligence (AI) to enforce intellectual property (IP) rights, such as improved detection of copyright-infringing content, design recognition and faster detection of trademark misuse. Conversely, costs, lack of transparency, data-sharing issues and ethical considerations constitute some of the challenges of AI. The contribution concludes that while AI offers promising solutions, careful piloting and attention to ethical, moral, and legal boundaries are essential before increased adoption.

I. INTRODUCTION

A. OBJECTIVES AND AIMS FOR THE STUDY.

1. This contribution is based on the research study *Artificial Intelligence and Intellectual Property Rights Enforcement*, which was commissioned by the Intellectual Property Office of the United Kingdom in 2021 to evaluate whether and how artificial intelligence (AI) can be used to track and trace intellectual property right (IPR) infringing goods, as well as to assess the potential use of AI by those infringing IPR.

2. The project aim was to review and collate existing literature and to capture the views of those with expertise and experience on the existing IPR enforcement landscape as to:

- how AI is currently used by right holders to protect and enforce IPR and
- assess threats from those infringing IPR.

3. The research covered five IPRs: patents, trademarks, designs, copyright and, notably, trade secrets.

B. METHODOLOGY

4. The project involved a two-phase process including:

- A critical examination of the AI and IP enforcement literature relevant to the five IPR under consideration, produced by government, academia and industry to identify core themes and outcomes to enable.

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

– This allowed for the creation of a questionnaire used as the basis for an extensive range of interviews with relevant stakeholders across industry, enforcement agencies, academia, legal practitioners and the judiciary to capture fresh and current insights of the current issues.

C. DEFINITIONS

5. At the outset, it was important to carefully define the terminology used, given the proliferation of definitions for AI.

6. The clearest and most succinct definition of AI as "human intelligence exhibited by machines", was provided by co-author of the study and AI expert Professor Kevin Curran.

7. Our research focused on the subset of AI, known as narrow AI, in the form of machine learning (ML). ML enables the creation of systems "that can learn from experience to find patterns in a set of data" and thus are able to infer or predict an outcome, even if the processes involve a few challenges as well as opportunities the identification of which were the main focus of our original study. Other relevant expressions mentioned in the contribution include:

– Narrow AI is the only form of AI that exists today and is trained to perform a single task, and unlike general AI, cannot operate outside of that defined task[1]. According to IBM "any other form of AI is theoretical" and even OpenAI's ChatGPT is a form of Narrow AI given it is "limited to the single task of text-based chat"[2].

– NLP (natural language processing) involves the ability for computers to understand text and spoken words similarly to human beings.

– Non-transparent AI (also known as black box AI) cannot be inspected in the same way as systems with a full audit trail.

– Neural networks, a subset of ML, are key to deep learning algorithms, using training data to learn and improve accuracy over time to enable high-speed data classification.

II. RESEARCH FINDINGS

A. MAIN OPPORTUNITIES

a) Copyright

8. There is an opportunity for increased use of AI tools in copyright enforcement, especially given certain apparently successful automated anti-piracy systems.

9. As a filtering tool, AI helps to identify infringing content and reduce human workloads, but it needs accurate and adequate training data. YouTube's Content ID is an example of an apparently successful AI tool as researchers have found it to be "working relatively well to

[1] IBM Data and AI Team (October 19, 2023), Understanding the Different Types of Artificial Intelligence, available at: https://www.ibm.com/blog/understanding-the-different-types-of-artificial-intelligence/.

[2] Ibid.

remove apparently infringing content from YouTube”[3], even though its success rate is not 100 per cent.

b) Designs

10. With regard to designs, improved image recognition capabilities could help identify potential infringements. Anti Copying in Design (ACID) maintains a databank of over 300,000 designs (including unregistered designs), which could provide data to train an AI to recognise infringing designs.

c) Trademarks

11. AI tools could help trademark enforcement analysts, if trained on very large datasets, freeing up human resources. There is scope for further development of enforcement solutions in close cooperation with consumer-facing online platforms that deploy AI tools for monitoring content.

12. For example, a new range of tools provided by the European Intellectual Property Office (EUIPO) offer track-and-trace solutions, risk analysis systems and use of AI/ML in detecting suspicious and potentially abusive domain name registrations.

13. AI could play a part in enforcing rights implicated in different types of cybercrime and in detecting counterfeits as an aid to human actors.

d) Trade Secrets

14. Trade secrets, especially for AI-related inventions, need enhanced protection against misappropriation. Security measures such as AI-based techniques, including neural encryption techniques, may offer greater protection.

e) Summary

15. Detection of copyright infringements is the most common example of AI use in IPR enforcement at scale, provided robust training datasets are available. If implemented similarly, AI could be also used to identify infringements of designs and trademarks, thereby reducing human resources.

16. Intellectual property analytics could improve the discovery of relationships, trends, and patterns of IPR infringement for improved enforcement decision making.

17. AI can only improve and become more accurate and faster, detecting patterns in a far superior manner to humans.

18. Overall, AI is a useful filtering tool and an aid to human analysis in speeding up the processes of identifying infringing content.

[3] Joanne E. Gray and Nicolas P. Suzor (2020), Playing with machines: Using machine learning to understand automated copyright enforcement at scale, Big Data & Society, available at: https://doi.org/10.1177/20539517209199.

B. MAIN CHALLENGES

a) Copyright

19. There are concerns about the costs and resources involved in using automated tools for enforcement against copyright infringements. Such tools may be beyond the means of many SME right holders, who mainly rely on collective management organizations and trade bodies to enforce their rights.

20. Automated anti-piracy systems are opaque and reliant on hard-coded automated rules using dynamic, potentially unpredictable, and non-transparent algorithms for decision making.

b) Designs

21. AI tools could help interrogate registered design databases. However, AI may not help identify infringements of unregistered designs or those reliant on copyright.

22. Apart from existing databases, such as the one maintained by ACID, the costs involved in using AI to identify infringements benefits large firms owning portfolios of designs.

23. The enforcement of registered and unregistered designs must consider the use of computer-aided design (CAD) and AI-generated designs, especially where unregistered design rights are used to train AIs.

c) Trademarks

24. Trademark enforcement is hampered by data-sharing issues between industry, government and enforcement agencies that inhibit the use of automated tools at scale.

25. Enforcement groups struggle to extract clean data from infringing websites and collate effective large data samples for the training of AI.

d) Patents

26. AI use in enforcing patent rights needs to combine a blend of human and technological knowledge.

27. The complexity of language involved in the application for patents as well as the complexity, cost and effort of taking legal action are challenges to enforcing patent rights. In addition, restrictions on using evidence of reverse engineering in English court proceedings make infringement of certain patent rights difficult to prove.

28. AI-generated or AI-assisted IP infringements must relate to the actions of a legal ‘person’, and, as such, enforcement may need to be taken against those operating the AI.

29. Enforcement against infringement of patents relating to AI may be hindered due to uncertainties associated with ‘black box’ AIs[4] that defy human comprehension.

30. AI tools are perceived as insufficiently nuanced or adapted for patent law, which requires lateral thinking and interpretation.

e) Trade Secrets

31. Trade secrets enforcement is impaired by the perceived risk of public disclosure during court proceedings , and therefore infringement issues are commonly settled out of court. Enforcement of trade secrets is also impaired by uncertainty around what may legally constitute a trade secret.

32. AI is seen as one of relevant factors involved in the increase of cyber thefts of trade secrets, which in turn requires new AI and ML tools to combat the cyber-attacks.

33. There is also concern that AI could be misused to hack into and get hold of trade secrets as opposed to protecting them.

34. Trade secrets cover commercially valuable information not protected by patents or other IPRs, but enforcement depends on taking reasonable measures to keep such information secret as they are only useful for as long as they can be kept secret.

35. In this regard, AI is seen as less immediately useful, given the nuances and variety within trade secrets and the fact that they are not intended to be public facing in the first place.

f) Ethical Issues

36. The ethical limitations of using AI in IPR enforcement include the quality of (such as inadequate or incomplete) training data sets involved in the decision-making processes, as well as systematic and inherent human bias that could lead to unfair or incorrect decisions.

37. There are also currently imperfections in the technology itself, including the lack of transparency (especially as regards “black box AI”) and accountability as well as an incomplete knowledge of how the AI’s work.

38. There are also fears over the inflexible decision-making process involved with an AI that could lead to ‘over-zealous blocking’ of legal content.

g) Legal Issues

39. AI tools would need retraining to meet the needs of different IPR laws in different territories. There is also the fundamental challenge of maintaining GDPR compliance when AI training data involves using mass volumes of personal or sensitive data.

[4] It is challenging to understand how a black box AI model generates its predictions “because its inner workings aren't readily available and are largely self-directed. Just as it's difficult to look inside a box that has been painted black, it's challenging to find out how each black box AI model functions”; see Kinza Yasar and Ivy Wigmore, Black Box AI, available at: https://www.techtarget.com/whatis/definition/black-box-AI.

40. There is a danger of “bad actors” harnessing AI, such as the ability to re-upload content after it has been removed by takedown notices.

h) Summary

41. The main challenges are the quality and quantity of training data needed for the effective use of AI in IP enforcement, as well as the crucial ethical and moral issues involved.

42. An AI system is a resource-hungry process, and there is a clear link between the volume of data used by the AI and the accuracy of the results.

43. The volume, quality and currency of training data are a common concern. It is clear that training AI tools is time-consuming and requires constant updating.

44. Given the current limitations of AI as well as the ethical concerns, AI should currently only be an initial tool for flagging content to a human analyst for verification, rather than for enforcing IPR independently.

III. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

45. In the use of AI/ML in the enforcement of each of the five IPRs, the challenges outweigh the opportunities, mainly due to fundamental issues relating to the use of AI in the enforcement of patents and trade secrets.

46. There remain other concerns about the use of AI in IPR enforcement, and these include:

– Warnings around the common methodological issues relating to the use of ML in the quantitative sciences were highlighted in a 2022 Princeton study[5].

– The UK’’s long-running Post Office Horizon software scandal highlighted “the dangers of humans blindly accepting the output of automated systems as reliable evidence”. The former Law Society President Christina Blacklaws’ warned the Post Office case should “serve as a cautionary story for every organisation*”.* Similar issues could occur in other organizations that have reduced technology resources, outsourced critical expertise, and adopted less suitable auditing processes[6].

– The Australian government’s failed experiment with Robodebt, which the ACS described the ACS as an “AI Ethics Disaster”[7].

– the emergence of adversarial ML, where bad actors can exploit vulnerabilities to exploit AI systems and alter their behaviour to serve a malicious end goal. These attacks can involve poisoning (of the training data) or evasion attacks, many of which go unnoticed until there is a ML critical failure.

[5] Sayash Kapoor and Arvind Narayanan (2023), Leakage and the Reproducibility Crisis in Machine-learning-based Science" Patterns, available at: https://doi.org/10.1016/j.patter.2023.100804.

[6] John Thornhill (April 29, 2021), Post Office Scandal Exposes the Risk of Automated Injustice, Financial Times, available at https://www.ft.com/content/08f485bf-6cea-46d6-962c-46263aaec5f3.

[7] The ‘Robodebt’ system was designed to automate data matching of income discrepancies in the tax system and increased the number of assessments almost 40-fold from 20,000 to almost 800,000 each year. In 2017, the Commonwealth Ombudsman found issues with transparency, usability and fairness of the digital system.

B. RECOMMENDATIONS

47. We remain confident of the ability of AI /ML to offer scalable solutions to assist the enforcement of some, if not all IPRs under consideration. We also stress that AI/ML itself is constantly improving.

48. We cannot recommend the increased adoption of the technology without emphasizing the significant caveats described earlier.

49. As such, we recommend careful piloting of any new AI-based IPR enforcement system to determine whether the system design takes account of the above drawbacks and whether the technology is operating within the ethical, moral and legal boundaries to achieve its primary purposes.

[End of contribution]

AN INNOVATIVE APPROACH TO ANTI-COUNTERFEITING: ARTIFICIAL INTELLIGENCE-POWERED PARCEL INSPECTION FOR INTELLECTUAL PROPERTY ENFORCEMENT

Contribution prepared by Ms. Karolina Zhytnikova, Legal Manager, Brand Protection and Intellectual Property, Countercheck GmbH, Berlin, Germany[*]

ABSTRACT

Countercheck's anti-counterfeiting solution is based on an AI-powered technology, which helps to protect consumers from dangerous goods and to enforce the rights of the intellectual property owners.

Introduced in the very middle of the logistics chain, Countercheck's software is installed directly on the pre-existing hardware in logistics firms' sorting centres. It monitors all the parcels coming through the hub to detect and intercept the parcels potentially containing counterfeit products.

Outdated legal frameworks, not adapted to the exponential development of e-commerce, are a major challenge that Countercheck is encountering while establishing its business model. Rigidity of the mechanisms of seizure and destruction of counterfeit goods in postal parcel flows and lack of powers for efficient and prompt responses to counterfeiters operating in internal markets are damaging the effectiveness of anti-counterfeiting efforts.

Logistics companies increasingly adopt a zero-tolerance approach to counterfeit goods in their networks. Smooth collaboration between public and private sectors within all industry players will help to meet new challenges in the fight against counterfeits.

I. INTRODUCTION

1. The growing popularity of e-commerce during the pandemic established a new pattern of consumer behavior. This phenomenon drastically increased the volume of products consumers ordered directly from the e-commerce platforms and social networks. Not only genuine goods, but also counterfeit items are shipped to customers by postal means, posing a serious threat to their health and safety.

2. The wholesale distributors of non-authentic goods are also actively exploiting this distribution channel to stock up on counterfeits. Postal shipments offer not only a cheaper and easier delivery, but also reduce the risk of interception by law enforcement authorities due to the random check of consignments. Moreover, in the event of an interception, the loss incurred by counterfeiters is relatively small compared to the quantities typically transported in trucks and containers. Those are the main reasons for the popularity of postal parcels or express shipments among counterfeiters.

3. Recognizing the challenges described above, the logistics industry, law enforcement authorities and intellectual property right (IPR) holders highlight the importance of automating the process and intelligent preselection of suspicious consignments from the entire parcel flow.

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

II. COUNTERCHECK'S ARTIFICIAL INTELLIGENCE TECHNOLOGY IN THE FIGHT AGAINST COUNTERFEIT GOODS

A. CONTRIBUTING TO THE INTEGRITY OF THE SUPPLY CHAIN

4. To tackle counterfeiting, AI technology might be used in multiple ways. This includes, for example – well-known and widely used approaches in pharmaceutical, tobacco and automotive industries – traceability (track-and-trace) solutions. They allow manufacturers and their legitimate suppliers to authenticate genuine products and detect disruptions at various stages in the supply chain. These technologies help IPR holders monitor in real time the life cycle of the genuine product and possible diversions and alterations of the secure codes in the market.

5. The main principle of the Countercheck solution is to use AI technology with a focus not on the genuine product, but on the analysis of the entire commerce flow. The aim is to isolate high-risk profile parcels, containing potentially counterfeit items, and to provide IPR holders and law enforcement authorities with a broader real-time picture of the movement of IP-infringing products (i.e., new roads, entry points, transit countries, etc.). Countercheck technology helps identify the hotspots and focus enforcement efforts for maximum efficiency.

B. ENHANCING THE EFFECTIVENESS OF ANTI-COUNTERFEITING EFFORTS

6. Countercheck's AI technology is directly introduced in the supply chain in logistics sorting centers. It allows automated control with reduced human interactions on the entire parcel flow and selectively disrupt it for IP-infringing goods only, without blocking all other legitimate products.

7. This detection process consists of multiple steps:

- The system extracts all the information from the outside of a parcel without analyzing its content/interior.
- The AI algorithm analyses more than 141 criteria without direct intervention in the parcel and takes the decision whether to block a consignment for further examination.
- If the risk assessment system indicates that the parcel potentially contains a counterfeit item with a probability of 80 per cent or more, it instructs the hardware to sideload the parcel to a separate, dedicated chute.

8. Using the latest machine learning technologies, the “risk profile” of each parcel coming through the sorting belt is established in 0.6 seconds. This allows for an efficient detection of potential counterfeits without disrupting the operations in the hubs and causing delays in parcel delivery.

III. CHALLENGES OF THE CURRENT LEGAL FRAMEWORK FOR IMPLEMENTING ARTIFICIAL INTELLICENCE-POWERED TECHNOLOGY

A. “DOMESTIC” PARCEL FLOW

9. At the European level, Regulation (EU) No. 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning Customs Enforcement of Intellectual Property Rights and Repealing Council Regulation (EC) No. 1383/2003 (hereinafter referred to as Regulation No. 608/2013) gives Customs authorities extended powers to fight counterfeits at the borders of the European Union.

10. In contrast to the commonly held opinion that most counterfeit goods are produced outside the European Union and are imported to EU countries from abroad, a large amount of counterfeits is produced[8] and/or assembled on European soil.

11. Unfortunately, national legislations across European countries do not always provide for effective mechanisms and powers to enable law enforcement authorities to deal with counterfeits in the internal market, especially for the “domestic” parcel flow. A positive example is France[9].

12. In France, the IPR holder may not only file an Application for Action (AfA) based on EU Regulation No. 608/2013, but also one based on the French Intellectual Property Code. This AfA makes it possible to monitor goods in the national territory. In other words, goods may be detained even though they have been cleared by customs and are in free circulation.

13. As a matter of fact, this lack of control leads counterfeit wholesalers to favor postal logistic channels for the provisioning of local flea markets, street vendors, illegitimate shops, warehouses and factories as a B2B model.

[8] For example, an underground production site of counterfeit cigarettes in France was shut down by the French National Gendarmerie: https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-tobacco-products-worth-eur-17-million-seized-in-france.

[9] Article 66 of the French Customs Code grants customs authorities a right of inspection and access to the premises of postal service providers and express freight companies: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071570/LEGISCTA000006138845/.

B. SMALL CONSIGNMENTS PROCEDURE

14. Regulation No. 608/2013 also provides for a simplified procedure for the destruction of suspected IP-infringing goods, which does not require a prior court decision (Article 26). This well-known procedure for the destruction of small consignments of counterfeit goods without contacting the IPR holders is widely used by customs for the border control of B2C parcel flows from e-commerce platforms.

15. However, once these goods are customs-cleared or if they were produced in one EU country and then expedited to another EU country by postal means, this procedure of the simplified destruction for small consignments is no longer applicable. There is no harmonized EU legal framework on the matter, and only rarely have countries implemented advanced approaches on the matter in their national legislations. Therefore, in most cases, internal market interceptions of suspicious goods are a police prerogative. In order to proceed with the seizure and further destruction of counterfeit goods, law enforcement authorities (police) are required to open and follow the ordinary (i.e., not the simplified) procedure, no matter if one pair of footwear or a batch of 500 items of allegedly counterfeit products is detected.

16. The absence of an efficient mechanism for the seizure and simplified destruction of all postal consignments is one of the biggest legal challenges facing Countercheck in the implementation of its technology.

IV. A NEW STANDARD OF SOCIAL AND BUSINESS RESPONSIBILITY TOWARDS END CONSUMERS AND BUSINESS PARTNERS IN THE LOGISTICS WORLD

17. To conclude, it should be said that AI technologies are helping to make our work more efficient, and that automation of routine processes saves law enforcement authorities a lot of time. Nevertheless, another very important element should be taken into account for the further success of the combat against the illicit trafficking of IP-infringing goods. This element is collaboration.

18. Increasingly, well-known logistics companies include a zero-tolerance approach to counterfeit goods in their network as an element of compliance and increased business responsibility towards their business partners in the logistics world. Moreover, by doing so, they send a strong message to the community about their social responsibility towards consumers and their will to protect society from dangerous goods.

19. Through the Countercheck platform, logistics companies, IPR holders, customs and law enforcement authorities are connected to deliver a prompt and strong response to counterfeiters. Efficient identification of suspicious goods by AI technology, quick confirmation of counterfeits by IPR holders on the dedicated online platform (within 24 hours) and close contact with customs and law enforcement authorities contribute to the integrity of the supply chain.

20. Looking towards the future, we foresee even more collaboration between the public and the private sectors, as this is a necessary element of a fruitful fight against IPR crime. Notably, we expect some shifts in democratizing the possibility for the private sector to intervene in relevant activities in the context of the phenomenon of the “fragmentation” of the counterfeit flow, i.e., shipping of counterfeits in small, separate consignments rather than in bulk.

21. We also expect an adjustment of the outdated legal framework that would reduce excessive precautions that affect the timeline of destroying counterfeit goods, as well as the establishment of efficient procedures to combat counterfeits for the “domestic” parcel flow.

22. Lastly, the countercheck solution offers functions – such as an integrated risk analysis of entire parcel flow, a real time control of the supply chain and a rich source of intelligence for further investigation of criminal networks – that are necessary elements to tackle new challenges in the fight against counterfeit goods. Only joint forces of all stakeholders in the brand protection industry will result in more powerful impact and will allow to create a safe ecosystem where there is no space for counterfeiters.

[End of contribution]

ARTIFICIAL INTELLIGENCE IN THE MUSIC INDUSTRY: ITS USE BY PIRATES AND RIGHT HOLDERS

Contribution prepared by Mr. Graeme Grant, Vice President of Global Content Protection, Universal Music Group, Hilversum, The Netherlands[*]

ABSTRACT

This contribution outlines Universal Music Group's (UMG) views on artificial intelligence (AI), focusing on its responsible use amidst deep concerns about intellectual property (IP) infringement. As a leader in the music industry, UMG employs AI for various applications, including a variety of uses from a marketing aid to a creative tool. While AI holds great potential for innovation and expansion, generative AI also poses great risks – not only to creators but to broader society, as well. For example, generative AI's deepfakes and other fraud also threaten individuals' privacy and consumers' safety. The contribution delves into growing unauthorized activities, such as using AI to mimic artists and generate fraudulent tracks and the unlicensed training of AI platforms on musical works. These unauthorized uses are increasingly prevalent across digital platforms, posing challenges in IP enforcement and raising concerns about the future integrity of artists' work. UMG concludes that AI can serve the interests of artists and creativity if used responsibly, but that it is a significant threat, if used irresponsibly.

I. BACKGROUND

1. Music is a story told through a harmony of expression and emotion. Songwriters and artists tell their stories in their own narrative and in their own voice. Through their music, they are sharing experiences that most of us will never have and taking us places that we will never go. Their creativity is the soundtrack to our lives. And without the fundamentals of copyright, we might not ever have known them.

2. Universal Music Group (UMG) is home to a broad array of music-related businesses, including in recorded music, music publishing, merchandising and audiovisual content, among others. Featuring a deep catalogue of recordings and songs across every musical genre, UMG identifies and develops artists and songwriters, and produces and distributes critically acclaimed and commercially successful music around the globe.

3. Committed to artistry, innovation, and entrepreneurship, UMG fosters the development of services, platforms, and business models in order to broaden artistic and commercial opportunities for the artists and create new experiences for fans.

4. UMG embraces artificial intelligence (AI), just as it did other technology innovations over decades. It uses AI for marketing purposes and gathering insights to grow artists' audiences, as well as fueling the creative process in studios and optimizing production. In fact, UMG holds several AI patents2.

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

5. Some newer AI technologies, especially “generative AI”, which has exploded over the past several months, present both opportunities and major risks for the creative community. AI can enable cutting edge tools that enhance human creativity for those artists that desire to use it. But some uses of AI bring great risk.

6. If used without respecting artists’ rights, generative AI technology poses risks to the creative community and the content it creates.

II. INFRINGING USES OF ARTIFICIAL INTELLIGENCE IN THE MUSIC INDUSTRY

A. UNAUTHORIZED TRAINING OF ARTIFICIAL INTELLIGENCE PLATFORMS

7. Some AI platforms are being illicitly trained on copyright-protected content, infringing the rights of creators. Following this training, they are used to further infringe these rights by creating output utilizing this content. In virtually every case, these platforms have not sought, let alone received, authorization. To the contrary, they typically seek to avoid any transparency as to their use of the musical works while using these infringements to further their own business.

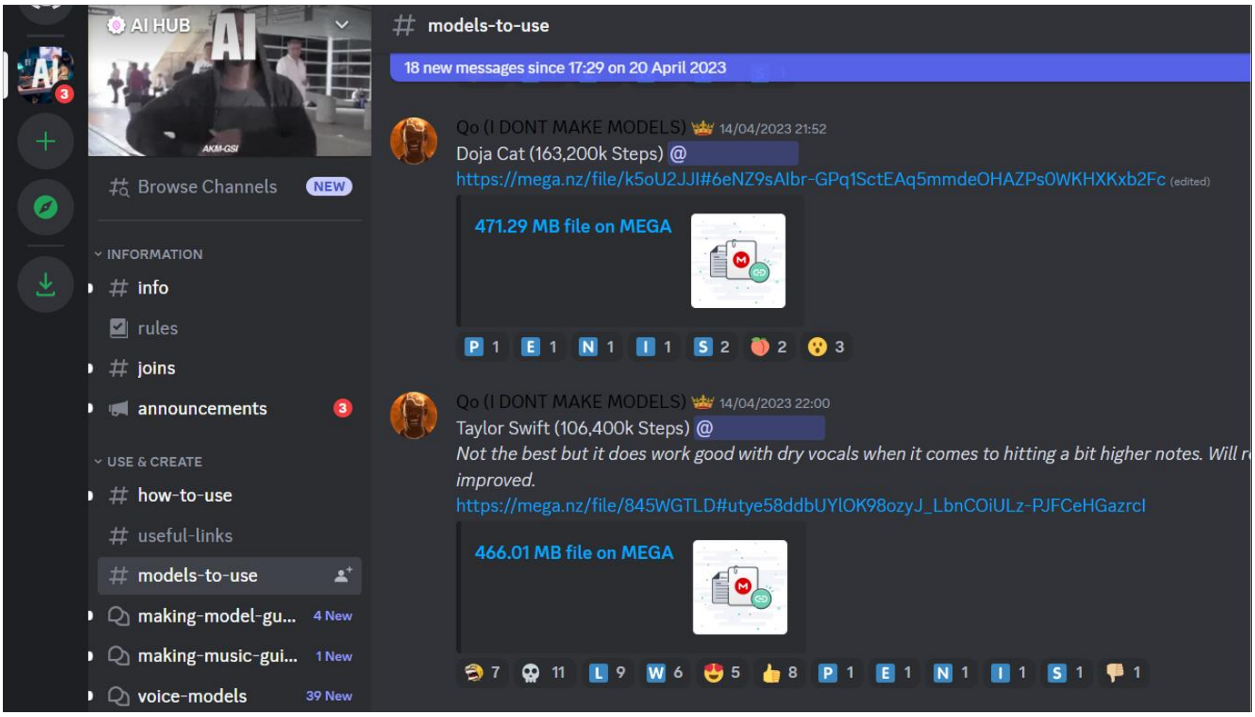
8. Over the past year, UMG has observed a significant increase in the utilization of AI to produce tracks that mimic the unique style and voice of the artists. Dedicated online communities are emerging, not only to create and distribute these fraudulent tracks, but also to provide comprehensive tutorials that guide individuals through the entire process of this unauthorized activity as well as tools – such as bots – which automatically perform AI vocal cloning processes. Since August 2023, the number of AI-generated uploads to user-generated content platforms implicating our rights has grown 175 per cent. Roughly 47 per cent of the notices sent thus far were triggered because a UMG master recording was detectible in the underlying vocal or instrumental; the remaining were violative of a musical/literary work copyright, trademark or a right of publicity claim.

9. Emerging technologies known as “Source Separators” are leveraging AI to isolate vocal and instrumental stems from master audio recordings (UMG uses this technology to support its artists). These separated elements are subsequently used to train sophisticated AI models. The use of UMG’s master recordings either as a whole or in part without authorization or a license represents a copyright infringement. This relatively new form of infringement synergizes with older methods, such as stream ripping. Stream ripping is where the audio component of an audio-visual work is extracted (typically from a licensed platform such as YouTube) and reproduced. This circumvents the technical protection measures applied by licensed streaming platforms to prevent unauthorized use of the content and breaches the platforms’ terms of use. The subsequent ‘ripped’ content serves as the input for these source separation algorithms.

10. Digital service providers (DSPs) and user-uploaded content (UUC) platforms are frequently exploited by AI creators to publish and monetize their creations, often including unauthorized use of copyright-protected works – including album artwork, master recordings, compositions, lyrics – or artists’ registered trademarks (such as their names and logos). While some infringers may face account suspensions or removals, they can often establish new accounts to perpetuate their unlawful activities. Further aggravating the issue, these infringers can engage in stream manipulation and royalty fraud by artificially inflating play counts and streams to unjustly boost revenue at scale, at the expense of artists and legitimate right holders.

11. In the preceding months, UMG has noted with concern that the community engaged in IP infringement has demonstrated alarming agility by modifying their techniques. Initially, during the primary growth phase of generative AI infringement, it was possible to secure the removal of unauthorized content predicated on existing copyright laws where an AI-generated vocal was

mixed over our underlying master recording without authorization. As the growth continued, AI has been used to create content featuring an artist's vocal clone but where the master recording is not as apparent in the output creating greater challenges in the removal of this content.



models-to-use

18 new messages since 17:29 on 20 April 2023

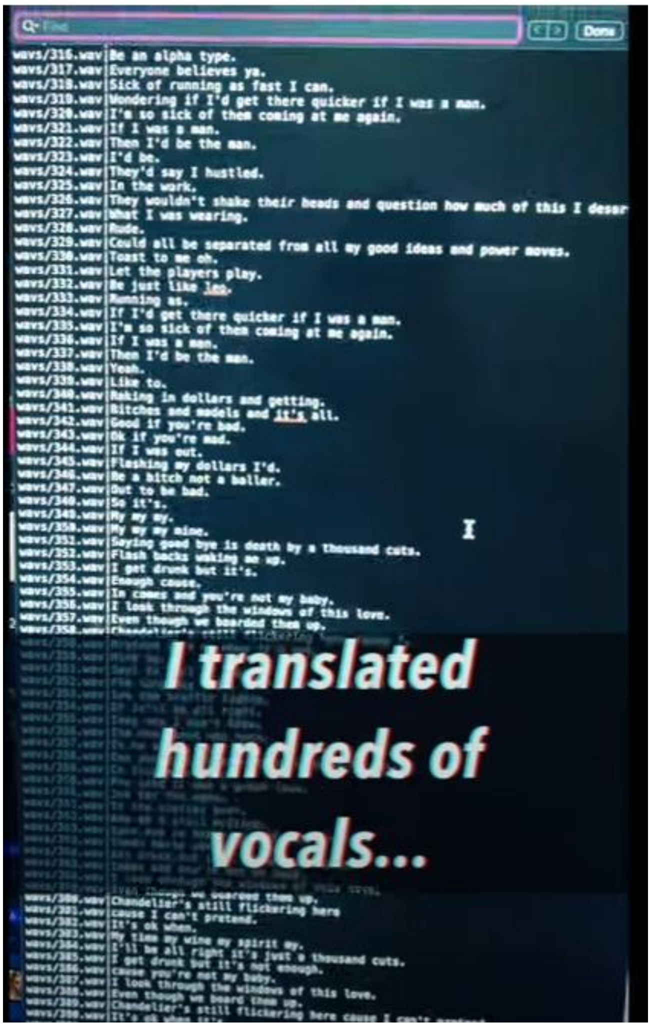
Qo (I DONT MAKE MODELS) 14/04/2023 21:52
Doja Cat (163,200k Steps) @[redacted]
https://mega.nz/file/k5oU2JJI#6eNZ9sAlbr-GPq1SctEAq5mmdeOHAZPs0WKHXKxb2Fc (edited)
471.29 MB file on MEGA

Qo (I DONT MAKE MODELS) 14/04/2023 22:00
Taylor Swift (106,400k Steps) @[redacted]
Not the best but it does work good with dry vocals when it comes to hitting a bit higher notes. Will r
improved.
https://mega.nz/file/845WGTLD#utye58ddbUYlOK98ozyJ_LbnCOiULz-PJFCeHGazrcl
466.01 MB file on MEGA

B. ARTIFICIAL INTELLIGENCE VOCAL MODELS

12. Some AI vocal models have been illicitly trained on UMG's copyrighted collection of audio recordings, lyrics and cover art. Additionally, specialized music generators have similarly exploited UMG's copyrighted musical works. These unauthorized activities frequently rely on stream ripping. Once these models are fully trained, they are often disseminated through social communities on platforms like Discord and Reddit, and repositories such as GitHub and Hugging Face. They are often accompanied by complete and comprehensive tutorials on how to employ these models to generate new, derivative works.

13. Figure 1 shows the unauthorized use of a copyrighted UMG work to build a vocal model. Note each line of the song has been split into individual sound files in order to map the sound to specific words.



```
wavs/316.wav|Be an alpha type.
wavs/317.wav|Everyone believes ya.
wavs/318.wav|Sick of running as fast I can.
wavs/319.wav|Wondering if I'd get there quicker if I was a man.
wavs/320.wav|I'm so sick of them coming at me again.
wavs/321.wav|If I was a man.
wavs/322.wav|Then I'd be the man.
wavs/323.wav|I'd be.
wavs/324.wav|They'd say I hustled.
wavs/325.wav|In the work.
wavs/326.wav|They wouldn't shake their heads and question how much of this I deser
wavs/327.wav|What I was wearing.
wavs/328.wav|Rude.
wavs/329.wav|Could all be separated from all my good ideas and power moves.
wavs/330.wav|Toast to me oh.
wavs/331.wav|Let the players play.
wavs/332.wav|Be just like leo.
wavs/333.wav|Running as.
wavs/334.wav|If I'd get there quicker if I was a man.
wavs/335.wav|I'm so sick of them coming at me again.
wavs/336.wav|If I was a man.
wavs/337.wav|Then I'd be the man.
wavs/338.wav|Yeah.
wavs/339.wav|Like to.
wavs/340.wav|Raking in dollars and getting.
wavs/341.wav|Bitches and models and it's all.
wavs/342.wav|Good if you're bad.
wavs/343.wav|Ok if you're mad.
wavs/344.wav|If I was out.
wavs/345.wav|Flashing my dollars I'd.
wavs/346.wav|Be a bitch not a baller.
wavs/347.wav|Out to be bad.
wavs/348.wav|So it's.
wavs/349.wav|My my my.
wavs/350.wav|My my my mine.
wavs/351.wav|Saying good bye is death by a thousand cuts.
wavs/352.wav|Flash backs waking me up.
wavs/353.wav|I get drunk but it's.
wavs/354.wav|Enough cause.
wavs/355.wav|In comes and you're not my baby.
wavs/356.wav|I look through the windows of this love.
wavs/357.wav|Even though we boarded them up.

wavs/380.wav|Chandelier's still flickering here
wavs/381.wav|cause I can't pretend.
wavs/382.wav|It's ok when.
wavs/383.wav|My time my wine my spirit my.
wavs/384.wav|I'll be all right it's just a thousand cuts.
wavs/385.wav|I get drunk but it's not enough.
wavs/386.wav|cause you're not my baby.
wavs/387.wav|I look through the windows of this love.
wavs/388.wav|Even though we board them up.
wavs/389.wav|Chandelier's still flickering here cause I can't pretend.
wavs/390.wav|It's ok when it's
```

Figure 1 - Training a vocal model

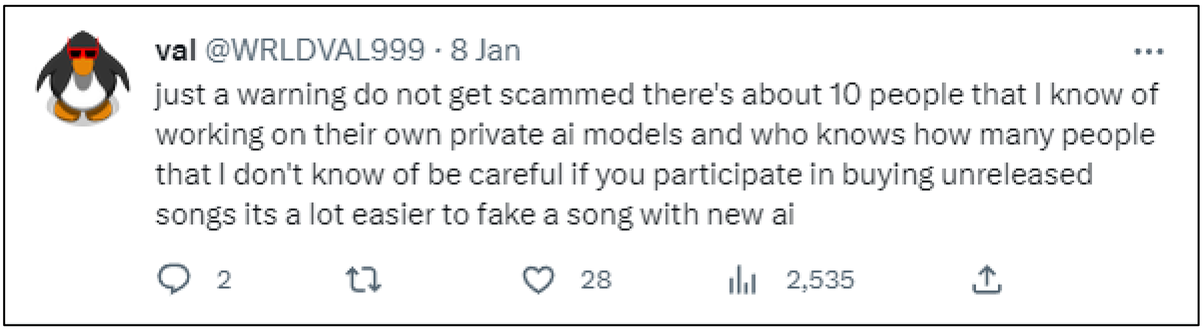
14. To give another example, one online community has created a spreadsheet containing over 100 pre-trained vocal models, relating to specific artists, that have been uploaded to services like Megaupload and Google Drive and can be downloaded and used by anyone of their 15,000 members.

15. Such vocal models were used to create a fraudulent track called *Heart on My Sleeve* which imitated the voices of Drake and The Weeknd and was uploaded to DSPs. The original track contained a sample from a UMG-controlled track called *No Complaints* by Metro Boomin, which was removed on the basis of copyright infringement. A new version of *Heart on My Sleeve* was then uploaded to DSPs with the Metro Boomin sample removed, which was reported on the basis of trademark and name, image and likeness violations.

C. PRE-RELEASE FRAUDULENT TRACKS

16. Increasingly fraudsters are using AI to claim they have pre-release tracks which they then make available for sale. These individuals typically upload brief snippets of AI-generated tracks impersonating UMG's artists voices to popular leak sites, falsely claiming to have obtained the tracks directly from the artists through illicit means such as hacking, phishing or misrepresentation. Believing these tracks to be authentic, users often engage in 'group buys', pooling their resources to meet the fraudster's inflated asking price, which can range from

USD5,000 to 30,000. The users are often unaware that the track in question was not created by the artist, but rather by AI technology.

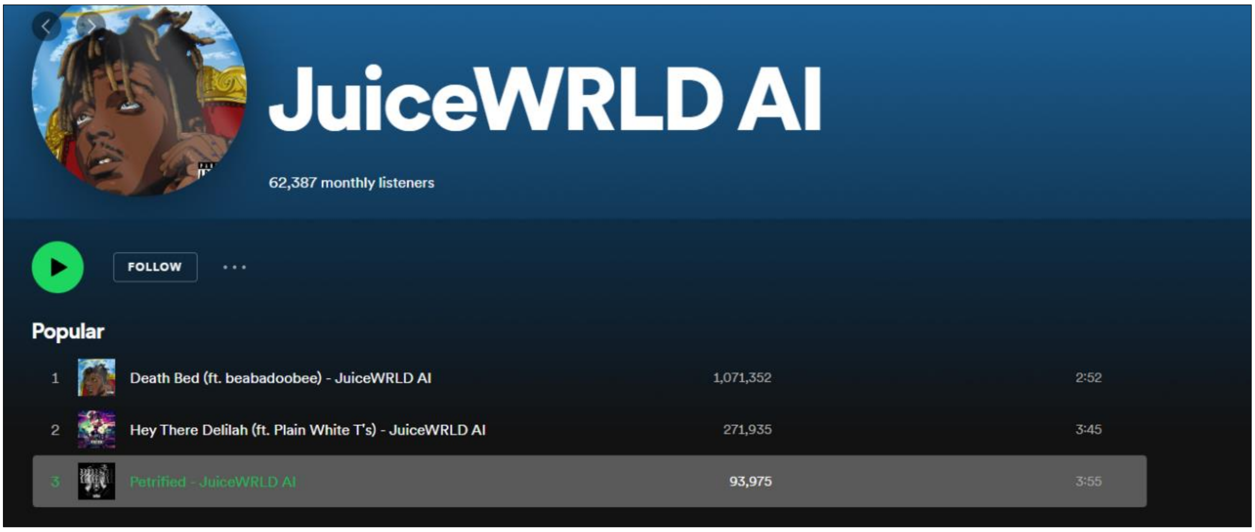


val @WRLDVAL999 · 8 Jan

just a warning do not get scammed there's about 10 people that I know of working on their own private ai models and who knows how many people that I don't know of be careful if you participate in buying unreleased songs its a lot easier to fake a song with new ai

D. FRAUDULENT TRACKS ON DIGITAL SERVICE PROVIDERS

17. Individuals that create fraudulent tracks from pre-trained AI models will use DSPs such as YouTube, Spotify, Deezer or Apple Music to generate revenue. They use aggregator services to upload the fake tracks to DSPs and claim full rights without acknowledging any use of the copyrighted content in either the finished track or the AI model used to mimic the artist. The royalties generated by ‘plays’ of the track on DSPs is diverted away from artists and right holders to the uploader of the fraudulent track (see the example below for JuiceWRLD).



JuiceWRLD AI

62,387 monthly listeners

Popular

1	Death Bed (ft. beabadoobee) - JuiceWRLD AI	1,071,352	2:52
2	Hey There Delilah (ft. Plain White T's) - JuiceWRLD AI	271,935	3:45
3	Petrified - JuiceWRLD AI	93,975	3:55

18. Tracks are often uploaded under fake artist profiles (Juice AI, Drake AI) to avoid detection by right holders and the DSPs themselves. On UUC sites – such as YouTube, TikTok and Instagram – tracks are uploaded using the real artist’s name and/or a hashtag in order to generate views, thereby increasing advertising revenue.

19. To demonstrate the growth of the problem, on one service provider during a 6-month period the number of AI uploads increased from around 50 to over 400 per day.

E. CYBERATTACKS FACILITATED BY ARTIFICIAL INTELLIGENCE

20. AI has increasingly become an instrumental tool in the orchestration of cyberattacks, representing a shift in the landscape of cybersecurity threats. Leveraging machine learning algorithms and other advanced computational techniques, malicious actors can automate the

process of identifying vulnerabilities within the systems and networks of record companies, thereby decreasing the time and expertise required to carry out their attacks. These attacks are often carried out with the purpose of obtaining pre-release works to be sold or to obtain stems which are then used to train AI models and create unauthorized works.

III. USE OF AI BY RIGHT HOLDERS

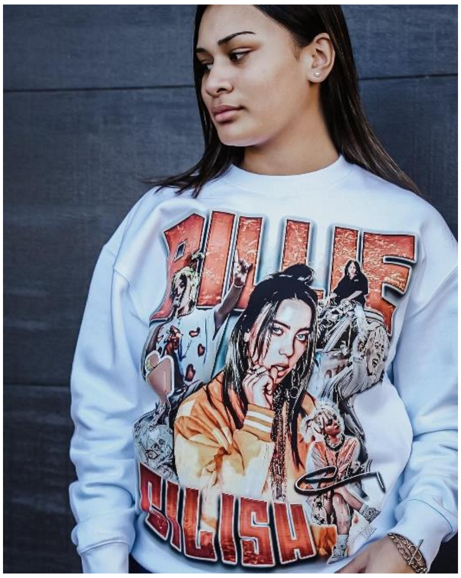
21. UMG has been thinking about AI long before an AI-generated recording imitating Drake and The Weeknd – both Universal Music artists – went viral and captured the attention of press and policymakers.

22. In November a new Beatles recording "Now and Then" was released which used AI to extract from an old demo recording a John Lennon vocal of such quality that it could be used in this new recording.

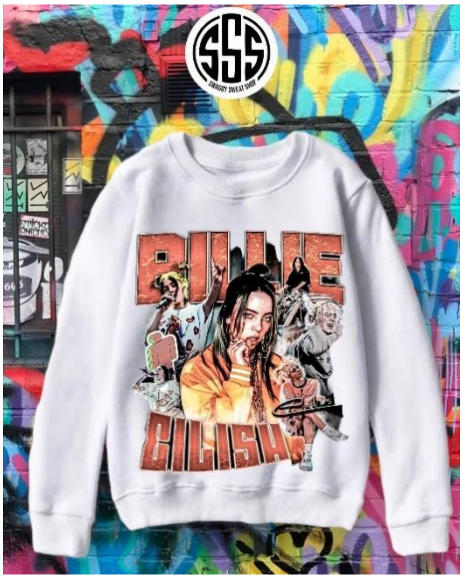
23. One of UMG's companies, Ingrooves, has three patents involving AI to assist with marketing independent artists. AI has also long been used as a tool in the studio, for example, with Apple Logic Pro X to generate drum tracks or Captain Plugins to generate chord progressions. UMG also uses AI regularly as a tool to assist in creating Dolby Atmos immersive audio music.

24. The UMG security team uses AI to protect the employees, artists and stakeholders against cybersecurity threats which are vast in number and growing in sophistication.

25. The UMG content protection team uses AI models to help in the classification of infringements based on a title, to create an infringement score based on metadata and to use image recognition to detect physical counterfeits and unauthorized uses of our brands and logos. As an example, sellers of infringing products will use original images but from different angles, in different sizes and colors or on different materials. AI image recognition is able to detect that these images are based on the same underlying image thereby increasing the detection rate. For example, AI was able to search for the "Billie Eilish" trademark and accurately read the words in the images of the counterfeits below, and this was despite the visual distortion in example 1.



Example 1



Example 2

26. To date we have detected and removed over 200,000 listings of counterfeit / unauthorized merchandise valued at over USD$45m+.

27. The UMG technology team uses AI to help making UMG's catalogue more easily searchable and discoverable, thereby supporting the internal teams, and augmenting the commercial opportunities for UMG artists.

IV. ARTIFICIAL INTELLIGENCE REGULATION

28. AI is a great technology when employed responsibly – and one that UMG uses in every stage of music development.

29. Public policy concerning AI is in its infancy internationally. Initiatives to regulate AI are underway in the United States of America, the European Union (EU) and the United Kingdom.

30. UMG endorses the commitments made by the G7, including in the May 2023 Hiroshima Leaders' Communiqué. The Communiqué and Declaration emphasize (1) "multi-stakeholder" participation in the development of AI standards that prioritize fairness, transparency, and adherence to existing laws; (2) commitment to "human-centric and trustworthy AI"; and (3) continued discussion and analysis of how best to safeguard intellectual property (IP) rights, including copyright.

31. The EU's Artificial Intelligence Act includes helpful proposals for government review of generative AI models before release, continued assessment of those models, recordkeeping provisions, transparency, labeling obligations and more. The Act also commits to many of the broad principles announced by the G7, including a focus on creator-led, fair, and transparent AI standards that, among other things, respect IP rights. The final version of the EU Act is now being discussed in tripartite negotiations ("trialogue"), and UMG hopes that the European Parliament's position on bookkeeping and transparency will be adopted.

32. It is essential that key entities in the generative AI chain keep detailed records, including of third-party materials, works or other protected subject matter used, alongside the basis on which they were accessed, and make this information available to parties with legitimate interests.

33. There are some policies that should be avoided. One example is text and data mining exceptions to copyright law as enacted in 2021 by Singapore. In addition, legislation in Japan, introduced in 2009 and amended in 2018, also includes too broad an exception which, while it is not unlimited and includes some protections for right holders, has the potential to cause confusion. Exceptions of this nature, in a world where generative AI swallows vast amounts of data in an uncontrolled fashion, run contrary to basic principles of fairness and the purpose of copyright law to reward creative effort. UMG is pleased that the UK explicitly rejected such policies last year in recognition of the irrevocable harm it would inflict upon its creative industries.

34. In general, UMG is of the opinion that current copyright legislation, if interpreted, applied, and enforced correctly, does not need to change. In selected territories, however, additional protection of personal rights (i.e., voice and likeness) may be necessary.

V. CONCLUSION

35. AI in the service of artists and creativity can create some wonderful tools, which we use in every step of music creation. UMG works together with numerous platforms, companies, artists and creators who use AI in a responsible way.

36. AI that is used to undermine legitimate use of music, ingests music without permission to unjustly influence the relationship that fans aim to have with real life artists and creators, or worse yet, appropriates their work – or their name, image, likeness, or voice – without authorization does not contribute to the music ecosystem.

[End of contribution]

THE USE OF ARTIFICIAL INTELLIGENCE BY MERCADO LIBRE TO DETECT AND TERMINATE INTELLECTUAL PROPERTY INFRINGEMENT

Contribution prepared by Mr. Gustavo Luis Bertelli, Machine Learning Manager, Machine Learning Delivery and Technology, and Ms. Guadalupe Yamila García Crespo, Brand Protection Manager, Legal and Government Relationships, Mercado Libre, Buenos Aires, Argentina[*]

ABSTRACT

Various legal frameworks around the world address the limitation of liability of Internet intermediaries and the establishment of complaint mechanisms for the reporting of offers that infringe copyright or industrial property rights. In Latin America, however, only few countries have adopted regulations for that purpose.

This means that in seeking ways to prevent the listing of counterfeit products and maintain high standards for the quality of their services, e-commerce platforms operating in this region must contend with the challenges of self-regulation and the absence of safe harbors.

In addition, the implementation of industry best practices in this area calls for complementing the reporting mechanisms with artificial intelligence (AI) models to proactively and automatically detect infringing goods when listed for sale. This presents the additional challenge of analyzing the reports received from IPR owners to establish a reliable, continuous and up-to-date source of knowledge about such infringements. This document examines the approach being taken by Latin America's Mercado Libre platform.

In Latin America, the development of solutions to combat e-commerce listings of counterfeit goods has posed particular challenges. The focus of this contribution, which is not intended to be exhaustive, is on the mechanisms developed by Mercado Libre to automatically remove e-commerce listings of counterfeit goods from participating member sites and examines it from both legal and technological standpoints.

I. BRIEF BACKGROUND ON THE REGULATORY CONTEXT IN LATIN AMERICA AND THE REPORTING MECHANISMS DEVELOPED BY MERCADO LIBRE

1. The normative framework governing the liability of Internet intermediaries for IPR infringements of intellectual property rights (IPRs) has evolved in different ways across Latin American countries.

2. The first example of such a framework is found in Chile, with the amendment in 2010 of its Intellectual Property Law No. 17,336. Apart from introducing a system of judicial notifications for the removal of copyright-infringing content, the amendment also provided for extra-judicial applications, obliging intermediaries to simply notify sellers when infringements have been alleged. Since that date, Brazil, Paraguay and other countries have regulated the limitation of the liability of Internet intermediaries, requiring essentially a judicial notification to establish specific and effective knowledge for allegedly infringing content to be removed.

[*] The opinions expressed in this document are those of the authors and do not necessarily reflect the views of the WIPO Secretariat or its Member States.

3. In 2020, Mexico amended its Copyright Law, as a result of the United States, Mexico and Canada Agreement, to replicate an extrajudicial private-sector mechanism established in the United States of America under that country's Digital Millennium Copyright Act (DMCA), enacted in 1998.

4. At the same time, various judicial rulings have taken on board the criteria of effective knowledge through identification of allegedly infringing content, even in countries, such as Argentina, where despite the absence of specific legislation on the matter, the principle has been acknowledged in case law form the highest local courts.

5. As part of this dynamic, good practices developed by the e-commerce sector, in Latin America and elsewhere, gradually prevailed over what was mandated by law, and paved the way for the implementation of voluntary and self-regulatory measures by intermediaries.

6. Such voluntary measures, sometimes negotiated with other private sector actors and government agencies, have been framed under the guiding principle of not imposing a general monitoring obligation on intermediaries. Instead, they depend on the knowledge and experience of IPR holders committed to exercising their rights through notice-and-takedown mechanisms.

7. In that context, IPR infringements generally, and particularly where trademark-infringing products are listed on e-commerce platforms, can be identified through the notice-and-takedown mechanisms. In the case of Mercado Libre, this is accomplished by means of an exclusive reporting channel, called the Brand Protection Program (BPP), which the company makes available to relevant IPR holders.

8. The solutions developed by Mercado Libre to combat the listing of counterfeit goods are not limited, however, to that single reporting channel. The company has launched various initiatives to derive lessons from the reports received, permitting the detection of infringement patterns and the removal of fraudulent listings in the absence of specific reports – and in some cases working directly and jointly with particular IPR holders.

9. This is linked to the continuous evolution industry best practices as well as applicable legislation and case law. In this sense, notice-and -takedown mechanisms are now being complemented by e-commerce platforms' pro-active efforts of – including by Mercado Libre in the countries where it operates – to detect trends and patterns in the infringement on their sites.

10. The next step in developing this reporting system for IPR holders is to educate other platform users about the range of existing IPRs and how to avoid infringement in listing products for sale, respond to infringement allegations and demonstrate to IPR holders that the goods offered are original. In the case of Mercado Libre, an allegation of an infringement triggers an immediate suspension of the listing concerned, which an appeal or response from the seller is not sufficient to reactivate. It is the IPR holder who then analyzes the seller's response and decides whether the listing can be reactivated or must be definitively removed. Definitive removals then serve as inputs for the identification of infringement trends or patterns and decisions to sanction repeat offenders.

11. Now, given the widespread absence of regulations in Latin America on the liability of Internet intermediaries, and the absence of safe harbors for intermediaries seeking to justify the removal of presumably infringing content, the reports received from IPR holders play an important role, both as justification for such removal decisions and – in form of lessons learned– as the basis for pro-active measures. The following section examines the technical issues arising from the use of artificial intelligence (AI) for that purpose.

II. ARTIFICIAL INTELLIGENCE AS A TOOL FOR THE DETECTION OF COUNTERFEIT GOODS

12. According to the World Intellectual Property Organization “there is no universal definition of AI. AI is generally considered to be a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence. Machine learning and deep learning are two subsets of AI. In recent years, with the development of new neural networks techniques and hardware, AI is usually perceived as a synonym for ‘deep supervised machine learning’”[10].

13. The Ibero-American Data Protection Network, referencing the Royal Society, provides the following explanation in its General Recommendations for the Processing of Personal Data in Artificial Intelligence: “Although there is not one definition of AI, it can be affirmed that in its ample conception, it is an ‘umbrella’ term that comprises a variety of computational techniques and processes that seek to enhance the capacity machines have to develop algorithms, to create machine learning systems, and to reach deep learning techniques. Particularly, AI is related to the use of algorithms, which are a group of rules or a sequence of logical operations in order for a machine to make a decision or act in a determined way”[11].

14. The large volume of data involved in a platform like Mercado Libre offers multiple opportunities as well as challenges for the application of AI. As mentioned earlier, reports received from IPR holders through the BPP are not only a source of key lessons for human users but can also be used to form algorithms to identify patterns and behaviors indicative of irregularities, which in this context consist of counterfeit goods listed for sale.

15. To place this volume of data in perspective, Mercado Libre, at the time of writing, operates a platform in 18 Latin American countries that is used by more than 3 million sellers and generates 45 sales per second.

16. The work required to identify and remove listings of counterfeit goods on such a platform requires several teams composed of individuals with different profiles and training and the use of multiple processes – a detailed explanation of which exceeds the scope of this contribution. Examined here are only a few of the relevant criteria and flows to provide context and a better understanding of how AI and machine learning are used to detect listings of counterfeit goods.

17. Difficulties arise from three main situations. First, the volume of goods identified as counterfeit by IPR holders represents a minuscule fraction of current listings on Mercado Libre sites: only 0.11 per cent for the first half of 2023, according to the company’s latest Transparency Report[12]. This suggests that the level of learning derived from the analysis of IP infringement reports could be higher if IPR holders more actively used the BPP.

18. Second, one of the variables that could be used as an additional input for the process of detecting a counterfeit good is the market price for the original products, providing a benchmark for singling out significantly lower-priced listings. At least as a preliminary step, excessively low prices relative to reasonable benchmarks are normally indicative of counterfeiting. However, while important, price cannot provide the only basis for detecting counterfeit products. Transitory discounts and/or promotions are sometimes offered by IPR owners themselves, so

[10] WIPO, Artificial Intelligence and Intellectual Property, available at: https://www.wipo.int/about-ip/en/frontier_technologies/ai_and_ip.html#accordion__collapse__01.

[11] Ibero-American Data Protection Network (2020), General Recommendations for the Processing of Personal Data in Artificial Intelligence, available at: https://www.redipd.org/sites/default/files/2020-02/guide-general-recommendations-processing-personal-data-ai.pdf.

[12] Available at: https://www.mercadolibre.com.ar/institucional/comunicamos/noticias/transparency-report-first-half-2023.

prices alone can be misleading. Sellers of counterfeit goods may also align their prices with those charged for the authentic articles, to avoid either detection, or consumer perception of counterfeiting.

19. Lastly, infringers may try to evade detection by adapting product descriptions or other aspects of their listings to more closely resemble the originals. This suggests a need for continuous learning systems to detect new infringement trends in analyzing reports received from IPR holders through the BPP.

20. Predictive classification models are being constructed based on supervised learning to address such situations, establishing algorithms with features for the detection of infringement patterns based on listing titles, images, references to product trademarks, most widely reported product categories, seller behavior and other variables.

III. CONCLUSIONS

21. The development of automatic, AI-based processes helps simplify the analysis of large volumes of information and expand the results obtained through a manual revision of content. In the case of counterfeit goods listed on e-commerce platforms, such as Mercado Libre, the aim is to increase the number of removals of such IP-infringing listings. According to the company’s last Transparency Report, proactive removals through the use of AI accounted for 87 per cent of all content removed based on IP infringements, with only 13 per cent of such content removed in response to particular IPR holder reports.

22. Infringers, however, continue to employ increasingly sophisticated practices to list counterfeit products online and pass them off as authentic articles. The use by IPR holders of private sector infringement reporting mechanisms, such as the BPP, will therefore continue to be essential to effectively combat the online sale of counterfeit goods.

[End of document]