Protecting Intellectual Property from Artificial Intelligence

Christian Demopoulos

Old Dominion University, Norfolk Virginia

CYSE 494: Entrepreneurship in Cybersecurity and Professional Studies

Professor Akeyla Porcher

June 21, 2023

Protecting Intellectual Property from Artificial Intelligence

Introduction

Artificial intelligence is a relatively new technology that serves the public in many capacities. While artificial intelligence does serve good purposes, it also poses enormous problems with copyright law and intellectual property. Artificial intelligence can also be used for great harm if left unregulated in its current standing. The problem with artificial intelligence is the type of information it can access. Artificial intelligence knows no boundaries with the information it can input and output. With this type of power, it leaves the question, "Does artificial intelligence output information using stolen ideas or purely original concepts?". Creators need protection for their ideas, inventions, writings, and concepts. Leaving artificial intelligence unchecked opens the door to many copyright infringements. Artificial intelligence requires a tool to protect intellectual property.

We know artificial intelligence is a problem because, just like an unlocked door, there will always be a risk that someone can break in. We need deterrents and corrective controls to stop intellectual property utilization. It is relatively easy to pull source material from an AI Chatbot. Creativity and innovation would be severely harmed by continuing to allow these types of practices. Some AI starter-up companies have ethical practices that go against piracy. However, with this technology being so advanced, we need more than a corporate company policy. I support innovation and parodying laws. However, blatantly stealing people's ideas is morally wrong. People's creative work needs protection and cannot be left to the goodwill of mankind. The current posture of artificial intelligence is creating a disaster for content creators and intellectual property owners. Original ideas must be protected.

My solution to intellectual property theft is creating a subscription-based service that provides a software suite that offers anti-piracy protection over artificial intelligence. First, the software suite would include a software application allowing subscribers to embed their intellectual property with metadata. This would, in turn, “tag” original content with indisputable identifiers that would allow unauthorized users to be easily found. Second, the software suite would include an algorithmic tool with a content filter to recognize intellectual property pulled from artificial intelligence platforms.

Lastly, the tool would include machine learning technology to actively search the web for “tagged” and older “untagged” creative content. When the tool finds unauthorized usage of intellectual property, a legal notice will be delivered to the offenders, similar to a copyright strike on YouTube. Utilizing this tool on paid content like movies, songs, and pictures would allow instant recognition and protect intellectual property from artificial intelligence. This tool protects intellectual property before and after it is published online. Using my service will hold people accountable and prevent people from pulling copyrighted material without being tracked or red-flagged.

I expect several barriers with my innovation. With so many advocates for artificial intelligence, I predict people will want to keep the government away from artificial intelligence. However, along with personal vendettas, there will be other challenges to overcome. Developing reliable algorithms that can recognize copyrighted content will take work. Creating a functioning machine learning platform will take time to perfect. Outsourcing a company to create a software application that can embed intellectual property will be pricey. Artificial intelligence will require intensive research and money.

Especially with copyright detection, there are bound to be false positives. We must ensure content is not mistakenly flagged, and information flow is not stopped due to incompetence. Lastly, we must be proactive and aware of pirates' new techniques to continue piracy. They will always be outlaws looking for new methods to break the law; our job is to stay on top of them. Continually analyzing pirates' new methodologies will promote our success. Allocating my software suite with proper funding and research will ensure favorable outcomes for future subscribers.

Scholarly Literature

A vital issue with artificial intelligence is the work it outputs and copyright distinguishment. Allowing artificial intelligence to operate in its current capacity has two main topics, "maintaining a 'freedom to operate,' or FTO, without violating third-party IP rights, and protecting investments in AI research and development." (DeCosta, 2017). This is true on so many levels. As artificial intelligence grows in popularity, we see how dangerous it can be. However, it is not illegal but treads on thin ice. Balancing artificial intelligence and protecting intellectual property is a complex compromise.

There are many legal complexities in artificial intelligence creating ideas. Who owns it, and is it copyrighted? These are fundamental questions to consider when greenlighting the usage of artificial intelligence. Using my software application from my software suite will allow society to determine intellectual property owners and prevent the theft of original ideas. Disclosure of original ideas in content creation is paramount. If there is a compromise in integrity, violators must be reported. “Under U.S. law, inventorship is the first point of analysis for determining ownership of IP” (DeCosta, 2017). Fortunately, my innovation includes automated reporting, which will disincentivize stealing intellectual property.

There are several legal risks surrounding artificial intelligence, ”Generative AI platforms using unlicensed works or generating unauthorized derivative works may face infringement penalties.” (Appel, et al., 2023). This is a crucial problem with artificial intelligence and is precisely what my software suite is designed to stop. People must be aware of artificial intelligence's capabilities and the potential associated risks. “Companies need to take new steps to protect themselves... and avoid generative AI tools that cannot confirm that their training data is properly licensed” (Appel, et al., 2023).

It is true that “Content creators actively should monitor digital and social channels for the appearance of works that may be derived from their own.” (Appel, et al., 2023). However, my software tool idea provides a remedy. The algorithmic tool I wish to design in the software suite saves end-users from doing the leg work. My innovation takes on the responsibility of protecting intellectual property by scanning the web for unauthorized usage. Moreover, Appel (2023) makes convincing points that anything generated by artificial intelligence should have “proper licensure”. Ensuring artificial platforms practice due diligence in protecting intellectual property is a noble cause. This motion, while applaudable, is unrealistic to expect without federal legislation. This is precisely where my innovation falls into play. Until there is some form of protection against artificial intelligence, my product will fill in those shoes. My product suite works for the little man and mitigates risk from predatory artificial intelligence users.

Nowak-Gruca dives into the "algorithmic ghostwriter" describing how artificial intelligence has evolved so much that others are taking credit for computer-generated ideas. This is a dangerous precedent as it desensitizes original ideas and encourages intellectual theft. "Nevertheless, the liberation of AI works from copyright law and their introduction into the public domain raises numerous doubts. Firstly, AI's texts and other works are created by being 'fed' with an enormous amount of data, including copyrighted data." (Nowak-Gruca, 2022). The narrative portraying artificial intelligence as the enemy is not far off. The direction of artificial intelligence is damaging innovation and creativity. This is why intellectual property needs to be protected from artificial intelligence.

Theft of original ideas has become not only extremely easy to accomplish but equally hard to regulate. "there is a real risk that AI systems, such as GPT-3, could write bestsellers by exploiting the works of existing authors, without providing any compensation for the right holders" (Nowak-Gruca, 2022). All this information from Nowak-Grucca supports society needing anti-piracy protection from artificial intelligence.

My software suite closes the gap with legalized robbery and returns original ideas to owners. It is only becoming more complicated to identify what is authentic and what is computer-generated. "First, it is unknown how to define algorithms capable of creating works of art or other works that may meet copyright protection conditions. The lack of a clear definition of artificial intelligence is the first and primary barrier in assigning legal subjectivity and the right to authorship of works." (Nowak-Gruca, 2022). Preventing the usage of intellectual property in artificial intelligence is for the best. Implementing my innovation will protect people's creative ideas and stop artificial intelligence from stealing intellectual property.

Another significant issue in protecting intellectual property is identifying original work. In artificial intelligence, deep fakes look natural and are hard to differentiate from real pictures. "It is near-impossible for casual consumers of images to authenticate digitally-altered images without a keen understanding of how to "read" the digital image." (Wagner & Blewer, 2019). Where is the limit if artificial intelligence can fool someone into believing a fake image is authentic?

Deep fakes are so dangerous due to their realistic attributes. Enabling technology like this with artificial intelligence creates a weaponized tool. Determining whether a digital asset is real or not is vital. People's reputation and hard work is on the line, and something needs to be done with artificial intelligence. "Much like Photoshop did for changing the public's understanding of trustworthy photographs, evolutions in artificial intelligence training and advanced computer graphics have resulted in a moment wherein altered video can seamlessly replace authentic video." (Wagner & Blewer, 2019).

This type of evolution is terrifying and demonstrates that we must limit artificial intelligence. Artificial intelligence is becoming too powerful and needs to be held back by the public. Just like deep fakes can persuade the masses, what proves intellectual property is not being stolen? We need a verification method to know what we are getting and to prevent theft. A solution to this complex problem includes incorporating my software suite innovation. Doing so gives the end user faith in what they see and alleviates doubt.

Authenticity goes a step further with artificial intelligence and escalates to fraud. With the capabilities of artificial intelligence being so advanced, it is becoming common to find fabricated works. “An important issue that we need to be alerted to is that intelligent generative models are used to forge images of scientific evidence and thus threaten academic integrity in publishing” (Gu, et al., 2022). Our scientists tell us they cannot distinguish real from fake science pictures. This concept is unbelievable as we become a society reliant on artificial intelligence.

In the scientific community, we see “fabrication of non-existent images (2) falsification or manipulation of existing images, and (3) plagiarism.” (Gu, et al., 2022). For situations like this, we need to verify the intellectual property owner. Artificial intelligence enables theft without protection from a middleman like myself. “it is difficult for editors and reviewers to find such frauds through visual inspection during the peer-review process. A user study indicates that scientific images generated by generative models are likely to deceive the judgment of human experts” (Gu, et al., 2022).

Knowing how cunning artificial intelligence is, why would anyone risk having their intellectual property stolen? It is too risky to leave it to chance, and the threat actors using artificial intelligence do not follow a set of aligning ethics. Our innovation provides the missing link in protecting intellectual property and ensures proper credit is due where owed. The software suite recognizes stolen or plagiarized intellectual property in the content filter. Companies need our innovation to ensure compliance on their end and to protect their assets.

Artificial intelligence is not going away, and its popularity is growing daily. Spreading awareness of this new technology will protect thousands of people's digital assets. "AI-enabled image fraud may pose serious challenges to the field of academic publishing. The difficult-to-detect nature, inexpensiveness, availability, and ease-of-use of advanced image generative models become major sources of threats when they are abused for scientific image fraud." (Gu, et al., 2022). Unfortunately, there is no direct method of preventing the abuse of artificial intelligence. Therefore, I propose that innovation be incorporated as soon as possible. As more time passes, more intellectual property is stolen, and it is harder to safeguard original ideas.

Artificial intelligence is growing exponentially, and usage is found worldwide. "At the same time, there are more and more problems with the unauthorized use of digital information for permission, and the copyright management and protection of digital information has become an urgent issue. Mistakers often steal data files that others have worked so hard to make without the permission of others for profit." (Che, 2022). Sadly, original ideas can be stolen easily due to this new, invasive technology. This type of behavior cannot continue.

Similar to our innovation, Che proposes watermarking intellectual property. This is a fantastic idea and streamlines protecting people's original work. "Digital watermarking technology is a digital product security protection technology, and it is an important branch of information hiding technology. Some traces are hidden in the multimedia data, and digital integration is used to prove the author's ownership of his work, which is used to prosecute evidence of illegal infringement" (Che, 2022).

As Che mentioned inserting “tags” on intellectual property will best deter theft. Fortunately, our software suite innovation proposes to accomplish this with the same methodology. Che (2022) further expands that “the detection of watermarks in multimedia files, the security of digital media information is guaranteed, and it has become an effective means to protect the intellectual property rights of digital media information.”

We can rest assured that these countermeasures are effective and accomplish our goal of protecting intellectual property. Last, there are several ways to watermark intellectual property. Some include visible watermarks, invisible watermarks, and fragile watermarks. In my innovation, we will use invisible watermarks because they are “generally invisible, but when needed, the watermark can be extracted from the original image through a special detection tool or software to prove the copyright of the original image.” (Che, 2022).

Another watermark our innovation could utilize is fragile watermarks. Fragile watermarks are very useful due to their protective nature. “When the original image is attacked, the watermark that cannot be detected by any change in any form is called a fragile watermark. It is mainly used to protect the integrity of digital media works and to prove the authenticity of images” (Che, 2022).

For our software suite innovation, embedding “tags: or watermarking people’s digital assets is key. Our goal is to make identifying the intellectual property as easy as possible. Additionally, to stop illegal usage of people’s digital assets. Since artificial intelligence is here to stay, our mission is to make stealing people’s intellectual property extremely difficult. Zhang et al. (2022) agree that the “most popular media copyright protection method is watermarking."

Watermarking is a very reliable means to protect intellectual property. Zhang focuses on images, but he still aligns with our innovation. His findings reinforce the need for my software suite innovation. “We introduce the IP protection problem for image processing networks. We hope it will help draw more attention to this seriously under-explored field and inspire more great works.” (Zhang et al., 2022).

Expanding Beyond Cybersecurity

The beauty of my design innovation is how it applies to many topics. While the nature of my product is based on cyber security, it is not just purely for cyber security majors. My software suite design protects intellectual property from artificial intelligence. Intellectual property covers a broad band of majors and fields of study. Preventing the unauthorized usage of intellectual property protects content creators and original content. Original content is not specific to one area.

For example, if a history major films an archeological sight, it would be in their best interest to ensure no one else could disperse their finding. Using my software suite would ensure that if anyone came across that video file, they would not be able to claim ownership. Using the software program from my suite would embed metadata into the video file to protect the video’s authenticity and verify the author. Additionally, if someone attempted to publish the history major’s video, my innovation would use our software suite’s machine learning technology to identify its presence and report the intellectual property violation.

If an art major created a one-of-a-kind art piece and sold digital copies, they would want royalties for its usage. My software suite can ensure such compliance. Using the software program from the suite will confirm the authenticity of the creator. Additionally, if the art is found being shared online, the machine learning technology would send alarms and alert the owner of the intellectual property violation. My innovation protects owners from intellectual property theft and allows future users to share content online without fearing losing credit for their hard work.

Whether you are majoring in history, art, science, math, computer science, or interdisciplinary studies, there is bound to be a digital file you will work with. My software suite ensures that intellectual property is not stolen through artificial intelligence, no matter the major. The problem with artificial intelligence is its massive impact on data consumption and the need for more boundaries. The lack of regulations opens up people's work and creditability being lost, due to a new technological advancement.

My tool is not specifically for cyber security majors, as every major involves some involvement with digital assets. The beauty of digital assets is their relevance in every major and promoting a standard solution for a vast amount of people. These reasons show why my software suite relates to an endless list of classes outside my major.

The Innovation's Effectiveness

Our innovative software suite will be deemed effective if it meets the consumer's expectations. First, the software application portion should have a user-friendly graphic user interface. Also, the application should have minimal instructions to promote a plug-and-play experience. Second, the algorithmic tool needs to be able to identify data from multiple artificial intelligence platforms quickly. Third, our machine learning technology needs to adapt to changing techniques and methods used to steal intellectual property.

If our innovation is effective, it will be proven based on the continual usage of our software suite. Additionally, catching the majority of pirates stealing intellectual property promptly will show effectiveness. When people stop using our product, we must reevaluate our software suite and brainstorm methods to incentivize future buyers. Lastly, ensuring appropriate legal action is taken against violators will show our consumers that we care and that our subscription service is worth paying for.

From Innovation to Reality

Making our innovation a reality will depend on a few factors. First, the intellectual property we "tag" needs a well-funded software program that is easily traceable and efficient at tagging. Second, our algorithmic tool needs an intelligent content filter. The content filter must recognize intellectual property tags from our software when the software suite rolls out. Third, the machine learning technology needs to be able to find creative content in a timely manner. Massive delays need to be avoided. The machine learning technology must distinguish what is protected by our software suite and what is not.

Fourth, our subscription service needs enough companies for long-term investment. The research, data, and staff onboarding will be costly in the first phase of rolling out the software suite. A year of good sales will likely be required for our innovation to make even. Our innovation must maintain a consistent consumer base to continue operations. We must continually think of methods to sell our software suite and keep our subscribers. If any of these pillars fail, then the product will not succeed or last long on the product floor.

We need to see a continual basis of copyright infringement and intellectual property violations for our innovation to stay relevant to consumers. If there is a decrease in violations, this would indicate that the benefits of our entire software suite are no longer necessary. From a strictly business standpoint, we always want to sell the complete product suite. However, if certain portions of the product suite are no longer relevant, a decreased price and smaller software suite option will need to be rolled out to remain consistent with the needs of our customer base.

Summary of Next Steps

Several insightful discoveries were made throughout the project that changed my views on entrepreneurship. First, know your target audience. Designing a product without knowing what your consumer base wants is extremely difficult. Knowing your people will make a significant impact on design innovation. Second, group feedback is crucial in identifying your weak points and lack of perspective. Collaborating as a team is crucial when you are creating a product.

Creating an innovation is not just simply thinking of an idea. Instead, it is a collection of ideas and critical thinking. A successful innovation must be thought out in detail and go beyond the surface level. A lesson I learned about the project was narrowing down the proposal concept early in advance. My project changed quite a few times due to a lack of understanding of the proposal. After some in-depth thought and discussion, I formulated a structured proposal idea.

Now that I have a well-thought-out innovation, I want to expand the reach of our software suite. Good advertising would do my innovation justice. Social media would be most beneficial to obtain a larger audience for my product. Better yet, a social media team for my innovation is needed. The only way to spread the news of our innovation is through mass online communication. From here, my business could build relationships with subscribers. Further down the line, we could produce massive contracts for our software suite to corporations at a bundled price.

In conclusion, completing this project allowed me to create a thriving, innovative idea that benefits content creators. This is all accomplished by our software suite, which protects intellectual property and regulates artificial intelligence. Brainstorming on this project allowed me to push my creative thinking to the limit. Finally, I have a greater perspective on entrepreneurship and what it would take to create a new product.

References

Appel, G., Neelbauer, J., & Schweidel, D. A. (2023, April 7). *Generative AI has an intellectual property problem*. Harvard Business Review. https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem

DeCosta, F. A. (2017, August 30). *Intellectual Property Protection for Artificial Intelligence*. Finnegan. https://www.finnegan.com/en/insights/articles/intellectual-property-protection-for-artificial-intelligence.html

Gu , J., Wang, X., Li, C., Zhao, J., Fu, W., Liang, G., & Qiu, J. (2022, July 8). *AI-enabled image fraud in scientific publications*. Patterns. https://www.sciencedirect.com/science/article/pii/S2666389922001039

J. Zhang, D. Chen, J. Liao, W. Zhang, H. Feng, G. Hua, & N. Yu. (2022). Deep Model Intellectual Property Protection via Deep Watermarking. IEEE Transactions on Pattern Analysis and Machine Intelligence, 44(8), 4005–4020. doi:10.1109/TPAMI.2021.3064850

L. Che. (2022). Application of Watermarking Algorithm Based on Artificial Intelligence in Service Outsourcing Intellectual Property System. doi:10.1109/AIE57029.2022.00036

Nowak-Gruca, & Aleksandra. (2022, January). *Could an Artificial Intelligence be a Ghostwriter?*. NIScPR Online Periodicals Repository. https://nopr.niscpr.res.in/bitstream/123456789/59280/1/JIPR%2027%281%29%2025-37.pdf

Wagner, T. L., & Blewer, A. (2019, July 19). *"The word real is no longer real": Deepfakes, gender, and the challenges of AI-Altered Video*. De Gruyter. https://www.degruyter.com/document/doi/10.1515/opis-2019-0003/html