December 16, 2019

United States Patent and Trademark Office, Department of Commerce

Re: USPTO Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation, 84 FR 58141

Dear Mr. Iancu,

The Center for Anti-Counterfeiting and Product Protection (A-CAPP Center) at Michigan State University appreciates the opportunity to weigh in on the questions posed by the USPTO regarding artificial intelligence and trademarks.

The A-CAPP Center is an independent, interdisciplinary evidence-based hub, housed in the College of Social Science at Michigan State University, whose activities focus on research, education and outreach designed to assist in protecting brands and products of companies in all industries worldwide. Our primary mission is to conduct academic research in the areas of counterfeiting, anti-counterfeiting and brand protection that generates knowledge and practical outcomes to inform industry, government, law enforcement.

The following is a brief summary of our recommendations and responses to questions 7, 8, and 9, focusing on AI’s impact to trademark law and protection. However, in light of the general lack of research in this area, we generally recommend an increase of resources dedicated to studying the legal and practical impact of AI on intellectual property.

7. Would the use of AI in trademark searching impact the registerability of trademarks? If so, how?

We believe that the use of AI in trademark searching will impact registerability of trademarks in several ways: a) impacting the markets in which a business may decide to register its trademark, b) possible data leaks with the information gathered by AI, and c) who is controlling the algorithms used in the AI and what impact that will have.

(a). The use of AI may have an impact on the specific markets in which a business may decide to register its trademark. Practically, many small to medium size enterprises may struggle with this; having AI recommend a certain market to them based on certain parameters that may not be in there best interest or not fully informing them of a risk in that market. This risk exists with any technology being used for this purpose.

Further, it would be theoretically possible that an entire trademark could be created by AI if an algorithm was created to determine whether derivatives of marks can be created, used and registered. We agree that the creation of the trademark itself should not be allowed by AI and that a live human, whether an individual or a company should
still be required to file for registration, to keep the final decision with a human, as well as any legal liability.

8. How, if at all, does AI impact trademark law? Is the existing statutory language in the Lanham Act adequate to address the use of AI in the marketplace?

We believe that AI impacts trademark law in several ways: a) the issue of trademark violations, both from the brand owner’s perspective but also from either the civil infringer’s side/criminal side, b) deception of consumers or misleading of consumers, c) lack of any liability, standards or regulations

(a). Trademark Violations. In regard to trademark violations, AI is currently being used by many brands and technology or security providers to scour the internet to do takedowns of infringing posts or goods. In theory, this allows infringing posts to be taken down at a greater rate than a manual process and the AI can be taught in an iterative way. The flip side, as we have seen through our research and with many prior technologies, is that whatever technology can be used by the brands or their agents to protect trademarks, can and will also be used to violate a company’s trademark.

With any use of AI with trademarks, the brand or mark owner’s involvement is and should remain important and central, with human verification of the AI recommendations being done and verification of the authenticity of the marks.

In this case of advertising, marketing, or promotion of products and services, it should be incumbent on the creator of the AI to ensure that it is not violating another’s trademark or other intellectual property. The onus should be on the technology provider to ensure this is not happening, and perhaps secondary liability on the brand using the technology.

Conversely, from our extensive studies in criminology, once a criminal or civil infringer has access to AI they can create algorithms that do exactly the opposite of the brands. These algorithms can find weaknesses in an online space or patterns in takedowns that allow the infringer the opportunity to train their algorithm to initiate multiple postings with modifications to language, images or other key features with a speed and efficiency that individuals cannot match. AI can be used to actively scour platforms for brands and products, get into regulatory agencies’ websites, search for high sellers, run them against the database, see what’s protected and what’s not, and in theory choose other jurisdictions in which to register; it could be used to identify patterns between patterns that are trending and those where there are gap and create an infinite variety of potential postings and postings.

(b). Deception of consumers- Regarding deception of consumers in the online environment, the use of AI can add complication through its shift of the retail experience, making it more predictive, meaning that consumers are shown a preselected grouping of products based on a variety of set factors. For example, a consumer only sees the party whose branding is appearing on the website with whom they are building a trust relationship, i.e. an e-commerce platform, a search engine, a brand. What they do not see is the third party or the technology, which could be AI, in the background that is informing their decisions. In essence, they are creating a relationship with that
technology whether they are aware or not. A possible suggestion might be co-branding of the AI with whatever platform, search engine or brand is using it, in order to help consumer’s identify the source of the recommendations, but also with enforcement. It will also encourage technology companies to build a public brand.

Another question arises regarding whether is there a duty to inform consumers of what the AI finds. For example, should an AI driven search algorithm identify goods that are 85% suspicious is there a duty to inform the consumer of the high likelihood of the items being illegitimate? Furthermore, at what level of validity should such an procedure occur? Over time AI driven processes are supposed to learn, adapt, and become better at predicting particular outcomes based upon prior information. At what level of prediction is there a duty to inform consumers, or brand owners, about a potentially suspicious product? Finally, should a consumer decide to purchase a product after receiving a warning that the item has a high likelihood of being illicit do they forfeit claims for relief should the product fail to perform as intended? Alternatively, the question of how false positives (i.e., incorrectly labeling a genuine item as illegitimate) must be addressed such that legitimate trade and commerce are not unfairly restrained or impeded.

(c). Liability & Regulations. If AI theoretically can do anything to autonomously identify intellectual property violations or to market and promote a brand, product or service without violating another’s IP, there is still a learning and developmental curve for AI. There will never be a situation where there is perfect prediction, instead there will be a level or point when the prediction is suitable enough. The question is when is it suitable? Who defines or how should suitable be defined? If it does not reach the point of suitability, it can be an incomplete, reckless or even infringing recommendation and then liability needs to be an option.

Additionally, because there is no current industry standard, we recommend that some industry standards be developed that can show active compliance with creators and users of AI technology.

(d) Statutory Language of Lanham Act. “Intent” of the defendant is an important element in question when looking at the Lanham Act and how AI may interact with it. Regarding the “intent” under §1117(b) for the case of using a counterfeit mark, the defendant must have “intentionally use[d] the mark or designation, knowing such mark or designation is a counterfeit mark…”  With AI being used to make either purchasing decisions online, or registering trademarks, or any other recommendations around IP, there is the potential for this to be infringing, as mentioned above. An unanswered question will be the test of intent or willfulness. Can AI intend for something to happen? Is the onus on the user of the AI or the creator of the AI to not ‘intend’ for a counterfeit mark to be used?

---

Further, in §1117(e), the rebuttable presumption of willful violation includes “knowingly provided or knowingly caused” false information to be provided to those in the domain name registry or industry. The same rebuttable presumption should be created in respect to AI, in that if a person knowingly provides or feeds false or infringing content into the AI, or withholds information that would prevent the AI from recommending infringing activity to be a willful violation.

9. How, if at all, does AI impact the need to protect databases and data sets? Are existing law adequate to protect such data?

AI is generally seen as a way to improve efficiency and speed up processes, yet, these processes also create a substantial amount of data that must be retained and stored. Within these datasets there exists the potential to have a singular location that contains a wide range of sensitive information. Access to this information can be gained through the systems supporting the AI processes, which are generally maintained by humans who have legitimate access to software and physical systems. The role of contract work (e.g., the gig economy) and highly mobile technical employees must be accounted for as individuals can carry with them the information and tools needed to gain unauthorized access to sensitive systems and data. Furthermore, the likelihood of an unintentional transfer of knowledge or knowledge spillover increases as employee mobility increases.

For manufacturers, modular production processes that rely upon digitization of information are likely to be interconnected with systems that utilize AI to gain functional efficiencies within the business. While modularity is intended to keep sensitive information protected by allowing partner firms access to only small snipets of data/information, the use of common interfaces and systems create weakness that can allow illicit actors access to sensitive information. If modular production processes involve AI or if they utilize the same systems as AI, threats to sensitive data and information that are gathered through AI processes can come from unrelated, yet, networked or integrated, systems.

Finally, it is important to consider the low-tech responses to the evolution of high-tech systems and processes. While AI is intended to create efficiencies and produce substantive gains for organizations, the potential exists that a heavy reliance upon these new processes can shift guardianship attention and focus away from other low-tech spaces. It would be incorrect to assume that simply because a system or process is highly sophisticated that it has the ability to account for the weaknesses of lower-tech systems and processes. Rather, AI should be seen as a way to supplement and enhance existing guardianship mechanisms, not as a complete replacement for them.
Sincerely,

Dr. Jeff Rojek  
Director

Dr. Jay Kennedy  
Assistant Professor

Kari Kammel, Esq.  
Assistant Director, Education & Outreach