Intellectual Property Infringement by Artificial Intelligence Applications

Eran Kahana
Research Fellow, Stanford Center for Legal Informatics,
ekahana@stanford.edu

The growing capabilities and widening use of artificial intelligence applications (AI apps) in mainstream consumer devices (e.g., Siri on the iPhone 4S) are converging to poise interesting intellectual property challenges.[1] While currently the most sophisticated of these apps are, at best, in an advanced-alpha or early-beta version, this technology is fueled by innovation moving at an exponential rate. According to futurist Ray Kurzweil, in just eight years from now, AI will demonstrate intelligence levels that are indistinguishable from that of humans.[2] And it does not stop there. With that milestone behind it, AI is predicted to outsmart its biological counterparts and, within the lifetime of current tenth graders, a paradigm shift will be witnessed where the majority of intelligence is non-human.

How these hyper-intelligent capabilities translate into a capacity of replicating human-based IP infringement is the subject of this paper. I start by examining this question through a computational capability-continuum, propose a categorization of AI apps based on such capabilities and offer a glimpse into a legal framework designed to deal with the behavior of such apps.

The common denominator for all four levels of AI apps identified here is that they can be programmed with every datum of known IP law. Additionally, each of the more sophisticated app iterations can perform all of the functions of the lesser-sophisticated ones.

I start at the low-end of the intelligence/sophistication continuum, and this is where we find the Level A apps. While these apps vary in their query-response sophistication capacity, they are programmatically constrained to perform that specific operation and are incapable of operational variance.

Level B apps respond to user queries and commands relative to retrieving data from sources external to the host device (such as an iPhone). Examples of these sources can be websites and other apps resident on any mobile devices that have granted the necessary access rights (whether on a device level or app level). The Level B apps also feature infringement-minimizing instruction sets to fit various IP environments in which they are intended to operate.

Level C apps feature autonomous decision-making capabilities. The Level C app can, for example, dynamically evaluate and decide from what source and what data to retrieve and how most effectively to present it.

---

[1] While the emphasis here is on AI apps, similar concerns apply to cybernetic AI.

[2] This event is widely known as passing the Turing Test.

Finally, the Level D app manifests intelligence levels so sophisticated that it can identify and reprogram any portion of its behavior (in unpredictable ways); i.e., it has a self-awareness capacity and can create other apps without human involvement. The Level D can also use data it finds in any manner it decides, in ways that indistinguishably replicate (and even exceed) human behavior.

Current law does not support a finding of infringement that is independent of human involvement. If there is infringement, a human-based "smoking gun" is a prerequisite for liability and appropriate remedy. For example, certain web content is copied and misused through use of a spider. Liability is attributed and remedies are sought against the designer, master or both. Simple enough. In contrast, similar activity undertaken by a Level D app is activity and harm for which the law currently has no answer.

A default strict liability standard against the human developer/deployer is misguided for a number of reasons. Perhaps most significantly among these is that it is probable that (e.g., in Level D app cases) that individual could not have reasonably foreseen the infringement. Instead, I propose that an iterative liability (IL) standard be adopted. Under it, infringement inquiry can begin with the original developer/deployer, but where the facts indicate that the AI app behaved sufficiently independently, that individual should not be held liable.

Once we dispose with the human-centric side of the inquiry, we need a legal framework that can handle assigning liability and dispensing remedy vis-à-vis these hyper intelligent AI apps. We could take a pull-the-plug approach and conclude that any AI app that is deemed infringing will be summarily deleted. While that may be feasible in the short-run, there is no assurance this will work in the long-term, especially where Level D apps self-propagate and know how to evade detection. The proposed legal framework I describe in the paper comes in the form of a uniform act that is specifically designed to address activities by such AI apps.