Intellectual Property - New Developments in Intellectual Property Law

15:00 - 16:30 Tuesday, 1st September, 2020
Track International Law

368 Artificial intelligence, design law and fashion: who is the genuine designer?

Hasan Kadir Yilmaztekin
Justice Academy of Turkey, Ankara, Turkey. University of Ankara, Ankara, Turkey

Abstract

Artificial intelligence (“AI”) now infiltrates our lives. From Apple’s Siri to Tesla’s auto-driving car and Amazon’s Alexa, we live in a world of AI goods. The upsurge of these novel technologies is at the centre of public debate and policy considerations. Some segments of the society have vocally raised their concerns: “machines are taking over”.

When we talk about AI-generated designs, we instead focus on the fruits of innovation without paying heed to who the designer is. Designers invest a lot of talent, time, and finances into designing and creating each article of clothing and accessory, before they release their work to the public. Pattern drafting is the first and most important step in dressmaking. Designers typically start with a general sketch on paper; add styles, elements and colours; revise and refine everything; and finally deliver their design to dressmakers. AI accelerates this time-consuming and labour-intensive process. Take the example of fashion brand Glitch, aiming to reimagine dress design with the help of an AI technique called Generative Adversarial Networks (GANs).

Yet the full legal consequences of AI in fashion industry are often forgotten. An AI device’s ability to generate fashion designs raises the question of who will own the IP rights of the fashion designs. Will it be the fashion designer who hires or contracts with the AI device programmer? Will it be the programmer? Or will it be the AI device itself? Or will it be a joint work?

This study makes policy proposals for future design law legislation within the EU. It particularly suggests that AI-generated and AI-assisted designs be protected under design laws through devising of legal norm, which is built upon a three-step test, to single out the human designer(s) from the relevant actors around the AI device.

215 The Internet of Things at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers.

Cristiana Sappa[1], Guido Noto La Diega[2]

[1]Iéseg School of Management, Lille, France. [2]Stirling Law School, Stirling, United Kingdom

Abstract

The Internet of Things (IoT) has heralded a never-before-seen quantity of high-quality data. This includes both personal and non-personal data. Control over IoT data gives companies unparalleled power to influence consumers, policy makers, and the other stakeholders of the IoT's supply chain. The combination of analytics algorithms, the data goldmine structure and the output of data processes are regularly kept secret by businesses. Leveraging this portfolio of big data and trade secrets, IoT companies put in place practices that can negatively affect consumers, who are often unaware of them due to technical and legal secrecy. 'Technical' secrecy results from the opacity of the algorithms that underpin the IoT, especially when AI-enabled. 'Legal' secrecy, in turn, come from a combination of trade secrets and strategic contract management that keep IoT data practices secret. This begs the central research question of this article: how can consumers be empowered to counter IoT data appropriation?

Traditional consumer protection approaches are focused on pre-contractual duties to inform consumers. Their benefit to IoT consumers is limited by their reflecting a text-based paradigm, whereby information must be legible. This is not fit for the IoT, where displays tend to disappear and information is provided in audio or video formats. Consumer laws are drafted on the assumption of information asymmetries in business-to-consumer contracts, but they fail to account for the power imbalances that permeate IoT transactions. These power imbalances are exacerbated by control over a wealth of user data and corresponding granular knowledge of consumers' vulnerabilities, behaviors, and biases. This knowledge can be used to impose opaque practices on consumers; among these, IoT data appropriation by means of trade secrets plays a key role.

Therefore, an emergent concern is whether the law provides tools that effectively safeguard consumers' interests, in particular by ensuring substantial transparency as to the actual use of their personal data. How can this can be guaranteed, and the consumer empowered in a post-interface world of profoundly imbalanced relationships?

The answer can be found in trade secrets' exceptions and GDPR rights to access, data portability, information, and not to be subject to solely automated decisions.