Implications of Deepfakes on Copyright Law

Author Bio: Neeraja Seshadri is a final year law student at School of Law, Christ University, India. The author's interests include intellectual property law, technology law and competition law. The contact details are can be found here: https://in.linkedin.com/in/neeraja-seshadri-0b5150120

Introduction

Deepfakes are fabricated images, audios and videos made using artificial intelligence. The common method of generating deepfake content is by the use of generative adversarial networks. The genesis of generative adversarial networks can be traced back to 2014. They are algorithmic architectures which primarily consist of two neural networks. While the generator neural network generates new synthesized or fake data, the discriminator neural network tries to detect the same. The process is repeated until the discriminator neural networks cannot differentiate between the original and synthesized data. This adversarial training in machine learning has been considered to be one of the most interesting developments in the arena of machine learning.

Deepfakes have the potential to be extremely useful and dangerous at the same time depending on the purpose of its use. The technology has been used for legitimate purposes in many industries. It has been used in the health sector to train artificial intelligence to detect tumors⁵ and has been used in the entertainment sector to create parodies and resurrect dead actors.⁶ However, the prominent use of this technology has been for malicious purposes like harassment

¹ Chris Nicholson, *A Beginner's Guide to Generative Adversarial Networks (GANs)*, PATHMIND (Jul. 22, 2020, 11:35 PM), https://pathmind.com/wiki/generative-adversarial-network-gan.

² Ian J Goodfellow et. al, *Generative Adversarial Networks*, CORNELL UNIVERSITY (Jul. 22, 2020, 11:37 PM), https://arxiv.org/abs/1406.2661.

³ Jason Brownlee, *A Gentle Introduction to Generative Adversarial Networks (GANs)*, MACHINE LEARNING MASTERY (Jul. 22, 2020, 11:39 PM), https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/.

⁴ Yann LeCun, *Director of AI Research at Facebook and Professor at NYU on potential breakthroughs in deep learning*, Quora (Jul. 22, 2020, 11:42 PM), https://www.quora.com/What-are-some-recent-and-potentially-upcoming-breakthroughs-in-deep-learning.

⁵ Jackie Snow, *Deepfakes for good: Why researchers are using AI to fake health data*, FAST COMPANY (Jul. 22, 2020, 11:44 PM), https://www.fastcompany.com/90240746/deepfakes-for-good-why-researchers-are-using-ai-for-synthetic-health-data.

⁶ Robin Pomeroy, *This iconic filmstar will star in a new movie - from beyond the grave*, WORLD ECONOMIC FORUM (Jul. 22, 2020, 11:47 PM), https://www.weforum.org/agenda/2019/11/james-dean-cgi-deepfakes/.

of women in the form of revenge porn⁷ and for post truth politics.⁸ The legal implications of the use of deepfake content has been widely debated across various jurisdictions as they have an impact on laws relating to copyright, defamation, privacy, data protection and intermediary liability to name a few. The use of copyright law to battle the issues posed by deepfakes has been widely discussed in the recent past owing to the fact that social media platforms are ill equipped to deal with them due to the lack of requisite technology to detect them. Facebook, Amazon and Microsoft came with the Deepfake Detection Challenge to develop a technology to detect deepfakes.⁹ However, the winner of the challenge had developed a technology with only 65.18% accuracy.¹⁰ In this context it becomes imperative to evaluate fundamental questions with respect to the viability of resorting to copyright law to tackle deepfakes. Since intellectual property is a territorial endeavor, the article would throw light upon the Indian and the United States position.

Copyright as a vehicle for the regulation of deepfakes

The position of regulation of deepfakes under copyright law in the United States is ambiguous due to the fact that there is a possibility that deepfakes can be protected under the doctrine of fair use as enshrined in 17 USC §107.¹¹ The various considerations under this provision are the purpose and character of use including commercial nature, the nature of copyrighted work, the substantiality of copying of the copyrighted work and the impact it has on the potential market value of the copyrighted work. Under purpose and character falls the concept of transformative use the conditions for which were first laid down in Campbell v. Acuff Rose.¹² It was held in this case that when a new meaning or expression is found in a work even if a substantial part of the copyrighted work which is the heart of the copyrighted work is copied, the doctrine of fair use can be extended to protect the work. The potential effect on the market is also a significant factor

_

⁷ Giorgio Patrini, *Mapping the Deepfake Landscape*, DEEPTRACE LABS (Jul. 22, 2020, 11:50 PM), https://deeptracelabs.com/mapping-the-deepfake-landscape/.

⁸ Regina Mihindukulasuriya, *Why the Manoj Tiwari deepfakes should have India deeply worried*, THE PRINT (Jul. 22, 2020, 11:52 PM), https://theprint.in/tech/why-the-manoj-tiwari-deepfakes-should-have-india-deeply-worried/372389/.

⁹ Facebook, *Deepfake Detection Challenge Dataset*, FACEBOOK AI (Jul. 22, 2020, 11:54 PM), https://ai.facebook.com/datasets/dfdc/.

¹⁰ James Vincent, *Facebook contest reveals deepfake detection is still an 'unsolved problem'*, THE VERGE (Jul. 22, 2020, 11:56 PM), https://www.theverge.com/21289164/facebook-deepfake-detection-challenge-unsolved-problemai.

¹¹ The Digital Millennium Copyright Act, 17 USC §107 (1998)

¹² Campbell v. Acuff-Rose Music Inc, 510 U.S. 569 (1994); Patrick Cariou v. Richard Prince, 714 F.3d 694 (2013); Pierre N. Leval, *Toward a Fair Use Standard*, 103 Harv. L. Rev.1105,1106 (1989-1990).

that needs to be taken into account while evaluating cases of transformative use. ¹³ Deepfakes can be protected under the doctrine of fair dealing in many situations in the United States as an argument can always be made that the nature of the work is completely different from the copyrighted work and therefore the likelihood of it causing any harm to the potential market of the original copyrighted work is extremely low. Where deepfake content is slanderous and defamatory other legislations can always be resorted to for imposition of liability. The issue with respect to deepfake and copyright law arises with respect to legitimate use of this technology and in such circumstances it becomes difficult to regulate deepfake content when the fair use doctrine is extended. This can also lead to problems with notice and takedown as mentioned in 17 USC §512¹⁴ and 47 USC § 230. ¹⁵ The intermediaries may also be faced the issue of detection of deepfakes which in turn makes notice and take down a tedious process and this makes it difficult to impose liability on intermediaries.

Moral rights are the rights which protect the reputation of the creator of a copyrighted work and also entitle them to the right to be attributed to their work. ¹⁶ In the United States, moral rights are extended to visual arts only. ¹⁷ There have been concerns that this approach is not in compliance with the Berne Convention as required under Article 6bis which states that moral rights must be extended to all works. ¹⁸ Moral rights can however be resorted to when the copyrighted work is modified in a manner which is prejudicial to the interest of the creator of the copyrighted work and in the United States it can be extended to cases where visual arts are used in deepfake content. The exclusive right of modifying content to create derivative works based on the copyrighted work is covered under 17 USC §106. ¹⁹ An action for copyright infringement can be brought if it can be proved that the deepfakes are not covered under the fair use doctrine and is merely a derivative work. Further, even the right to reproduction under 17 USC §106 can be resorted to where tests like substantial similarity test, ordinary observer test, virtually identical

¹³ Rogers v. Koons, 960 F.2d 301 2d Cir. (1992).

¹⁴ The Digital Millennium Copyright Act, 17 USC §107 (1998).

¹⁵ The Communications Decency Act, 47 USC § 230 (1996).

¹⁶ Betsy Rosenblatt, *Moral Rights Basics*, HARVARD UNIVERSITY (Jul. 23, 2020, 11:47 PM), https://cyber.harvard.edu/property/library/moralprimer.html#:~:text=In%20the%20United%20States%2C%20the,of%20who%20owns%20the%20work.

¹⁷ Visual Artists Rights Act, 17 U.S.C. § 106A, (1990).

¹⁸ Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as revised at Paris on July 24, 1971 and amended in 1979, S. Treaty Doc. No. 99-27 (1986).

¹⁹ The Digital Millennium Copyright Act, 17 USC §106 (1998).

test, total concept and feel test and more discerning observer tests can be used to impose liability on the creator of deepfake.²⁰

The Indian position is that of fair dealing and is covered under Section 52 of the Copyright Act, 1957 which provides as an exhaustive list of what is excluded from being considered as copyright infringement. Since deepfakes are not included in this specific list it is easier to impose liability on the creator. Further Section 57(1)(b) of the Copyright Act, 1957 provides for the right of integrity as well as paternity. Protection is accorded against distortion, mutilation and modification of a copyrighted work. Furthermore, the right to create derivative work rests with the author as under Section 14 of the Copyright Act, 1957. Section 55 ²⁴ and Section 63 ²⁵ impose civil and criminal liability for violation of exclusive rights. Due to the existence of these provisions it also becomes easier to impose liability on intermediaries owing to the current legal position after Myspace Inc. v. Super Cassettes Industries Ltd ²⁶ and Section 79 of the Information Technology Act, 2000.²⁷

Copyright law can therefore be used as a regulatory tool with respect to deepfakes based on the position of law in each jurisdiction and in certain jurisdictions copyright protection can be extended to protect deepfakes. The ownership of this particular copyright must be extended to the person who uses the generative adversarial network technology to make the deepfake content as intellectual property is used to incentivize creativity to stimulate further innovation.²⁸ The legal personality of artificial importance is to be evaluated to better perceive this approach. The most important essential to accord legal personality to any entity is the requirement of will and the ability to hold rights and fulfill duties.²⁹ The primary issue that arises in the case of artificial

-

²⁰ Harney v. Sony Pictures 704 F.3d. 172 (2013); Steinberg v. Columbia Pictures 663 F. Supp. 706 (S.D.N.Y. 1987).

²¹ §52,The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).

²² Id. at §57.

²³ Id. at §14.

²⁴ Id. at §55.

²⁵ Id. at §63.

²⁶ Myspace Inc. v. Super Cassettes Industries Ltd, MANU/DE/3411/2016.

²⁷ §79. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

²⁸ WIPO, What is intellectual property?, WIPO (Jul. 24, 2020, 12:56 AM), https://www.wipo.int/about-ip/en/

²⁹ Bryant Smith, Legal Personality, 37(3) Yale L. J. 283 (1928).

intelligence is the dilemma around the concept of will due to the blackbox problem. 30 The black box problem is that an artificial intelligence is a machine and that it is impossible for human beings to comprehend the way an artificial intelligence perceives the world. In this context, it becomes difficult to understand what rights and duties would mean to an artificial intelligence system. Therefore it becomes difficult to come to a conclusion that the purpose that intellectual property rights have with respect to humans will be the same with respect to artificial intelligence. Therefore it would not be wise to grant copyright to the deepfake technology in itself. Further it needs to be taken into consideration that computer programs are considered to be literary works as required under Article 10 of the TRIPS Agreement. 31 In India computer software is considered to be a literary work under Section 2(0)³² and in the United States it is considered to be a literary work under 17 USC §101.33 Therefore, policy considerations and deliberations must be made with respect to deepfake technology being included under the ambit of literary works. In this light it becomes viable to accord copyright to the person who uses the technology to make deepfake content. If the deepfake content made does not fall under the ambit of transformative use and subsequently fair use then it can be considered a derivative work for which regulations for permissions from the owner of the copyrighted work may be created to ensure that their economic rights are not overlooked.

Conclusion

Deepfake technology is being widely used across the world and the amount of deepfake content generated is likely to increase at a rapid rate as various applications are being created to make the technology easily accessible to the masses. There are certain issues with respect to detection of deepfakes as there is no viable technology created in the current scenario which can effect intermediary liability and notice and takedown measures under copyright law. However, copyright law can still act as an effective vehicle for regulating deepfakes if it is tailored to meet the needs and standards of different jurisdictions. However, it is imperative to take note that no straightjacket formula can be created and enforced across the world.

_

Mathew Cress, The Black Box Problem, Artificial Intelligence Mania (Jul. 24, 2020, 1:05AM), http://artificialintelligencemania.com/2019/01/10/the-black-box

 $problem/\#: \sim: text = Because \%\ 20 the \%\ 20 human \%\ 20 brain \%\ 20 doesn, no \%\ 20 way \%\ 20 of \%\ 20 looking \%\ 20 inside.$

Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 3; 33 I.L.M. 1197 (1994).

³² The Digital Millennium Copyright Act, 17 USC §101 (1998).

³³ §2(o), The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).