AI and Deepfake Voice Cloning: Innovation, Copyright and Artists’ Rights

Harnoorvir Singh Josan

Fall 2023 cohort
About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub’s identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people’s lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

Mitacs
Introduction

AI is a discipline of computer science that allows machines to simulate some aspect of human cognition (Calo 2018). The mind-boggling developments made by AI in recent years have been the reason for the buzz around it. Most of the contemporary excitement is due to a particular sub-field of AI called machine learning. Machine learning refers to the ability of machines to recognize patterns in the training data and, thus, improve their performance in tasks over time (ibid.). The availability of massive amounts of training data and computational resources such as extremely powerful computers have led to breakthroughs in machine learning over the past decade (Sturm et al. 2019). The breakthrough events are not just concentrated in the information technology sector but have bled into other fields such as creative arts, health care, finance and so forth. Recently, the music industry has seen a rapid increase in AI-generated vocals where a song is produced without any actual input from the singer. In these cases, a technique called deepfake voice cloning is used. Deepfake voice cloning refers to when AI bots mimic speech patterns and cadence via exposure to the recordings of human speech (Houser 2019). One side effect of such clones is that they are easy to manipulate and can be used to spread misinformation online. In August 2023, an anonymous account posted alleged “leaked recordings” of the ex-president of Sudan on TikTok, which were later proved to be AI-generated, leading to confusion in a country already torn by strife due to civil war (Goodman and Hashim 2023). Due to this technology being novel, no concrete legal frameworks in the United States and Canada have yet addressed this issue. As more celebrities are falling victim to voice cloning, it is high time to consider the legal avenues of recourse (Wells-Edwards 2022). This paper will decipher the use of AI in creative fields, especially voice cloning techniques, look at some of the key cases that
pertain to this topic and provide some recommendations on policy developments that will prevent the illicit use of deepfake voice clones and assist celebrities in safeguarding themselves from any form of misinformation and disinformation campaigns.

Background

AI has long been used in the music industry but was limited to music and beat production as well as music distribution via streaming services (Sturm et al. 2019). AI voice cloning bots have recently infiltrated the recording industry. A simple Google search using the keywords “voice cloning” generates numerous results for voice cloning bots such as voice.ai, which boasts of generating realistic replicas of the original speaker’s voice in real-time for live streaming, group chats or gaming experiences.1 Some users have used this technology to clone the voices of celebrities and insert them into songs they created in order to garner more streams and views. A recent example of this is an AI-generated song “Heart on My Sleeve” — produced by an anonymous TikToker dubbed Ghostwriter977 — that was uploaded to major streaming platforms and quickly went viral on social media (Blackburn 2023). The song featured AI-generated vocals of two famous music superstars, Drake and The Weeknd, and was even submitted to the Grammy Awards’ Best Rap Song and Song of the Year categories (Das 2023). This is not the only example where the voice of a celebrity was used without their consent. Deepfake voice cloning AI models have also previously been accused of depicting a band cancelling its concert that had not actually been cancelled, showing artists endorsing things that they had never recommended and musicians bad-mouthing their fans, resulting in customer deception and undermining the public image of artists (Goldman 2023). Although voices are unique to individuals and are a key aspect of their personality, they are not copyrightable entities because copyright protects only original works of authorship fixed in any tangible form; the sound of a voice is not adequately “fixed” and, hence, cannot be owned by an individual.2 The lack of a copyright framework to prevent using someone else’s voice allows the users of voice cloning bots to use the replicas in any form without facing repercussions.

How to Ensure Voice Cloning Bots Do Not Violate Copyright

The song “Heart on My Sleeve” is not an isolated incident; techies have recreated Ice Spice’s “Munch” being sung by Drake, Beyonce’s “Cuff It” by Rihanna and Kanye West rapping Travis Scott’s “90210,” with fans showing they like such music (McGee 2023). If users can clone celebrities’ voices easily, it is not difficult for anyone to use the same technology to spread misinformation to portray these celebrities in a bad light. To prevent this from happening, there needs to be a framework that requires a substantial amount of vigilance and ensures that AI-generated music is produced in a way that provides fair compensation to the artists.

---

1 See https://voice.ai/voice-cloning.

2 Midler v Ford Motor Co, 849 F (2d) 460, 462 (9th Cir 1988).
The first step in the voice cloning process is training the model to produce the expected results (Koempel 2020). Training machine learning models to produce voice replicas requires a large amount of data, such as pre-existing music, audio recordings, interviews and so forth. Unless an exception applies, music used to train a model is generally protected by copyright (Sturm et al. 2019). Even if the user is prohibited from using the music recordings as training data, they can use a large pool of non-copyrighted data such as voice recordings, audio snippets from interviews and speeches to mimic the voice. Once the voice replica is ready, it may seem that the easiest legal avenue for a victim would be a lawsuit alleging copyright infringement of voice as it is a distinctive feature of one’s identity. Unfortunately, a victim of voice cloning cannot prevail in a lawsuit based on copyright infringement as the courts have already held in Bette Midler’s case that voices are not fixed in any tangible form and, thus, inherently uncopyrightable. Such a legal avenue is possible only if copyright frameworks are altered to allow for the copyright of voice. If a copyright infringement lawsuit is not an available option, some work can be done to ensure that training data is coming from a source that the voice supplier has approved.

Not all artists are reluctant to share their voices with AI bots. Some artists, such as Grimes, a Canadian synth-pop artist, have allowed the public to use their voices without worrying about copyright infringement or legal enforcement (Shanklin 2023). For such artists, there should be a common marketplace of training data that is not copyrighted, is legally owned by the artist and is free to be used for cloning voices. Only the lawful owner of music should be allowed to supply recordings to the archive. It can be the artists themselves or the recording labels who own any work. Such a bank could act as a government-controlled repository like Getty Images, but for audio recordings where all the stock recordings are available. This archive could provide a catalogue of various artists who have allowed the use of their voice and access to their music and audio recordings. There should also be a regulation for the voice cloning bots to accept training data only from that archive. This would also allow artists or asset management companies to charge for accessing their voice recordings if they want to. Having an archive of data provided by the artists themselves would ensure that users can create voice replicas of only those artists who do not have any objections, without having to worry about copyright infringement or legal enforcement. There should also be a requirement for the bots to automatically tag the output audio as AI-generated so it is easily identifiable and does not cause any confusion. YouTube is currently testing a tool called “Dream Track,” which is a voice cloning bot and will be used to generate songs using cloned voices of artists who have collaborated with YouTube and provided permission to use their voice (Savage 2023). YouTube also announced that it will start tagging any content generated by AI so that viewers can easily identify AI-generated content (ibid.). Although the initiative by YouTube is one step toward ensuring that voices are not used without the provider’s consent, it can be very disorganized and time-consuming for celebrities to grant permission to individual tools or bots one by one. If there was a bank or marketplace for all the bots, artists would only have to provide their consent once. If this repository comes into play, copyright frameworks could be adjusted later to allow an individual to succeed with a copyright infringement if a deepfake voice is created using their audio recordings outside of the bank of stock recordings.
Who Should Own the Final Product?

Protecting artists from having their music or audio recordings used to deepfake their voice without their consent is not the only problem in the process. Even if the clone is generated with the artist’s permission, the question of ownership of the end result still remains. In the United States and Canada, there are three fundamental criteria for granting copyright protection: “originality,” “work of authorship” and “fixed in a tangible form.” For a work to be original, it must be created independently by the author without the contribution of others and should be the creativity of the author without copying it from someone else’s work (ibid.). The original work does not necessarily have to be novel or innovative, but must be more than just mechanical or routine, which requires no creativity. In the case of AI-generated music being discussed here, just the vocals are mechanically generated, and the user has to perform all the other necessary steps such as lyric writing, audio editing, mixing and mastering. As the originality requirement is so low, most works including AI-generated music easily meet this requirement (McJohn 2015). The third requirement is that the generated work is “sufficiently stable to be perceived, reproduced, or communicated for a period of more than transitory duration.” As long as it is fixed in a tangible form, music generated with AI vocals meets this requirement for copyright purposes. The only requirement that poses a threat to the ability of AI music to receive copyright protection is the authorship. Copyright protection only applies to work with human authors. Although this requirement is not formally enshrined in the Copyright Act of Canada or the Copyright Law of the United States, the courts have refused to grant protection to works generated by non-human actors. Therefore, AI cannot be considered an author for copyright purposes despite being the most important player in the voice cloning process.

There are three candidates left for the authorship of the AI-generated works. One is the voice cloning software’s programmer, another is the user who trains the model and produces the final output, and the last is the artist whose voice is cloned using the audio recordings to train the model. Some authors have supported the claim of granting authorship to the programmers of AI systems, arguing that granting them the rights will encourage the growth of AI technology and systems (Hristov 2017). Some have used the same argument to support the authorship being granted to the end users of the software (Brown 2018). Given that in this case artists play an important role in allowing the use of their identity, they deserve to claim the authorship of the output. This would allow them to decide how and where their voice is used and receive fair compensation if used for commercial uses. Both the United States and Canada grant copyright protection to joint authors, given that each author is human and has contributed substantially to the work. The most equitable output is one that allocates joint authorship to both human and non-human actors (Grubow 2018). This will ensure that all the human

---

6 Naruto v Slater, 888 F (3d) 418 (9th Cir 2018).
7 Copyright Act, RSC 1985, c C-42; Copyright Law, supra note 5.
and non-human actors involved such as programmers, end users, artists and AI are compensated fairly and encourage the development of fair AI technology. Once the copyright framework is altered to remove the barriers to AI joint authorship, lawmakers should work to ensure that collaboration with AI is regulated (ibid.).

**Conclusion**

In the end, AI systems are not something that the public needs to worry about if proper safeguards are put in place. Deepfake voice cloning may sound like something that can be used to portray celebrities and artists in a bad light or steal credit by producing songs using their identity. However, if the users of AI and artists work together synchronously, and some changes are made to the copyright framework, a fair use model of AI can be ensured. The most important step is to ensure that the input data used is approved by the original author, performer or the artist. All the voice cloning systems should be required to input the training data only from a bank of stock recordings that are provided by the artists themselves. Once the model is trained and the final output is ready with the voice replica, it should be tagged as AI-generated so the general public can recognize it as such. To ensure all the involved actors get recognition and a fair share, ownership should be distributed jointly among programmers, users, artists and the AI. The current copyright framework in the United States and Canada does not grant authorship to non-human actors. Altering the copyright frameworks to allow for joint authorship of human actors and AI will allow the artists to be fairly compensated without hindering the development of AI technology. The laws to regulate the collaboration of humans with AI need to be implemented because AI systems, if used fairly, can foster creative intelligence, expand our knowledge and improve access to content.

**Acknowledgements**

The author would like to thank Brian Fauteux (University of Alberta supervisor) and Paula Martins (peer reviewer).

**About the Author**

Harnoorvir (Harnoor) Singh Josan is a computer science undergraduate student at the University of Alberta with a passion for innovation. Harnoor’s research with the Digital Policy Hub will centre on AI, music, and copyright policies in Canada and the United States, furthering his commitment to leave a meaningful impact in the technology and policy creation domains. Previously he worked as a product owner for an enterprise mobility management solution that merged his technical acumen with business insights.
Works Cited


