DEEPFAKES: LEGAL & REGULATORY CONSIDERATIONS IN NIGERIA

Augustine Eigbedion*

Abstract

It is often said that a tool is only as good as the hands of the one who wields it; same can be said of the novel digital technology known as "deepfakes". Deepfakes are hyper-realistic manipulated images, videos or other digital representations created by cutting-edge artificial intelligence tools. Whilst deepfakes could be highly innovative with an inherently creative and commercial value, this technology has been deployed in a socially harmful manner, as majority of deepfake demonstrations thus far (coupled with the reach and speed of the social-media ecosystem), have been employed to trigger misinformation, perpetrate fraud and undermine privacy concerns amongst other negative impacts. Although the technology hasn't gotten a foothold in Nigeria, same is however unavoidable when one analyzes it's possible use against the backdrop of the heavy reliance we now place on e-commerce, remote working, on-line learning, digital meetings and conferencing, artificial intelligence/machine learning tools and other frontier technologies, which until now were second-best choices in our daily interactions. The thrust of this paper is to examine briefly but lucidly, the possible legal and regulatory options that may be adopted in addressing issues arising from deepfakes in Nigeria.

Keywords: deepfakes, technology, law, regulation, Nigeria

I. INTRODUCTION

In recent times, the world has been awash with tons of altered videos depicting events of people doing or saying things they never said or being in places they never were. Known as "Deepfakes", this technology has been deployed to several ends. Whether it's a video of Barack Obama calling President Donald Trump a "*complete dipshit*"[1], or Mark Zuckerberg bragging about having "*total control of billions of people's stolen data*"[2], or the fictional character Jon Snow apologizing to fans for the somewhat unpopular ending to the tv series 'Game of Thrones'[3], the facts remain that the deepfakes phenomenon is on the rise.

In view of the vibrant social-media ecosystem that can spread content around the digital space with a simple mouse click, it is without doubt that despite the immense potentials of deepfakes, majority

*Augustine Eigbedion is a Legal Practitioner based in Lagos State, Nigeria. He can be reached via eigbedionaustine@gmail.com

[1] In April 2018 renowned US actor, comedian, and director, Jordan Peele collaborated with Buzzfeed Media to demonstrate the power of deepfakes by creating a video of former President Barack Obama (voiced by Peele) giving a public-service announcement about the dangers of deepfakes — an announcement that Obama never made. Available at <https://www.youtube.com/watch?v=cQ54GDm1eL0>. Accessed on 3rd April 2020

[2] In June 2019 a deepfake of Facebook founder Mark Zuckerberg surfaced online, wherein he appeared to seemingly give a sinister speech about Facebook's power to control billions of people's data. Available at < https://www.vice.com/en_us/article/ywyxex/deepfake-of-mark-zuckerberg-facebook-fake-video-policy>. Accessed 3rd April 2020

[3] Available at < https://www.youtube.com/watch?v=4GdWD0yxvqw>. Accessed on 3rd April 2020

of its demonstrations thus far have revealed how this technology has spread misinformation, triggered fraud and privacy concerns, and more importantly the threat it poses to our already vulnerable information ecosystem, thereby creating uncertainties about our shared reality.

At the time of writing this article, deepfakes have not been deployed in Nigeria, however, it is only a matter of time. The democratization of deepfakes through the surge of publicly available mobile applications and software tools easily accessible to anyone having a knack for genuine creativity or mischief, have sparked social and ethical discussions, and further raised a number of legal posers. Do victims (individuals and corporate entities) wrongly affected by deepfakes have any recourse in the law? What is the role of intellectual property in addressing creations from deepfakes? What is the best regulatory response to deepfakes in Nigeria? This article makes an attempt at proffering answers to the foregoing questions.

Part I of this article gives a general introduction of the concept and also statement of the problem; Part II examines the concept of deepfakes, the technology behind their creation, reasons for their growth and the challenges inherent in the technology. Part III explores the various uses of deepfakes, the downside when exploited for criminal and illegal use, and also where deepfakes are utilized for commercially creative ventures. Part IV gives an overview of how some of the existing laws and regulations (both civil and criminal) in Nigeria can be used in addressing the technology, whilst giving other possible measures address the rise of deepfakes. Finally, Part V gives remarks on the subject and concludes.

II. WHAT ARE DEEPFAKES?

Deepfakes are hyper-realistic images, videos and audios digitally manipulated to depict individuals saying and doing things that never actually happened.[4] Deepfakes surfaced to publicity in 2017 when a Reddit user posted videos showing celebrities in compromising sexual situations.[5] The appellation for the technology deepfakes itself is a blend of the terms "deep learning" and "fake". Essentially deepfakes rely on neural networks that analyze huge sets of data samples to learn to copy a person's facial expressions, mannerisms, voice, and inflections.[6]

Although content fabrication and decontextualization ("photoshopping") of still images has been the centerpiece of the digital society for quite some time now; a quick dive into history reveals that photography had long lost its innocence, as the art of 'photo-tampering' have been utilized by respected leaders as Abraham Lincoln or even dictators as Joseph Stalin who engaged the services of photo retouchers to cut his enemies out of supposedly documentary photographs.[7] Hence, the

[4] Bobby Chesney & Danielle Citron, "*Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*," 107 California Law Review 1753 (2019). Available at <http://dx.doi.org/10.2139/ssrn.3213954>. Accessed on 12th May 2020

[5] The said AI-generated videos display celebrities Scarlett Johansson and Gal Gadot having their faces mapped onto the bodies of porn actresses in action, thereby making it appear that the celebrities are actually performing live sexual acts.

[6] Mika Westerlund, "The Emergence of Deepfake Technology: A Review", Technology Innovation Management Review. Nov 2019 Vol 9, Issue 11

[7] Erin Blakemore, "How Photos Became a Weapon in Stalin's Great Purge", Available at < https://www.history.com/news/josef-stalin-great-purge-photo-retouching> Accessed on 2nd April 2020. The art of photo retouching was also adopted by Adolf Hitler, Mao Tse-tung, Benito Mussolini and a huge list of leaders.

steady rise of the manipulated videos of people now increasingly finding their way online and rapidly circulating across numerous social media platforms has generated concerns about deepfake technology by almost everyone aware of the technology and anyone who places reliance on audiovisual evidence.

Deepfake technology are primarily the product of an AI technique known as 'Generative Adversarial Networks' (GANs), namely two artificial neural networks working together to create impressively realistic images, video or sounds.[8] The key idea of GANs is to train two networks called the 'generator' and 'discriminator', together on the same dataset of images, videos, or sound, where the generator tries to produce images that would trick the discriminator into believing they were real. Simply put, the process involves feeding footage of two people into a deep learning algorithm to train it to swap faces.[9] Although initial research on deepfakes technology, disclosed that deepfakes usually require a large number of images to create a realistic forgery, however present research indicates that GANs can be trained on less information as researchers and even tech companies are already developing techniques to generate a fake video by feeding it only one photo such as a selfie.[10]

Audio sounds can also be deepfaked, to create "voice skins" or "voice clones" of people. In August 2019, the world witnesses the first noted instance of an artificial intelligence-generated voice deepfake used in a scam, when the CEO of a UK subsidiary of a German energy firm paid nearly £200,000 into a Hungarian bank account after being phoned by a fraudster who mimicked the chief executive of the firm's German parent company.[11] Furthermore, similar scams have reportedly used recorded WhatsApp voice messages in defrauding unsuspecting victims.[12] It is interesting to note that the deepfake technology can create convincing but entirely imaginary photos from scratch. One case was the fabricated senior journalist, "Maisy Kinsley", who had a profile on LinkedIn and Twitter, and supposedly worked for Bloomberg. Also, of note is the case of the Linkedin fake "Katie Jones", who purportedly worked at the Center for Strategic and International Studies, but was widely believed to be a deepfake created for 'mass-scale' spying operations, particularly on Linkedin.[13]

The rapid growth of deepfakes can be largely attributed to include : (i) development of large image databases, particularly with the active participation of hundreds of millions on several social media

---

[8] Edvinas Mesky, Aidas Liaudanskas et al, "Regulating Deepfakes: Legal & Ethical Considerations", Journal of Intellectual Property Law & Practice, 2020, Vol 15, No. 1 pg. 26

[9] Ibid

[10] Westerlund (n 6). Also, the newly developed Artificial Intelligence by Samsung Electronics lab in Russia can fabricate video from a single image, including a painting. Available at < https://www.cnet.com/news/samsung-ai-deepfake-can-fabricate-a-video-of-you-from-a-single-photo-mona-lisa-cheapfake-dumbfake/> Accessed on 3rd April 2020

[11] https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/. Accessed on 3rd April 2020

[12] Ian Sample, 'What are deepfakes – and how you can spot them'. Available at <https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them#img-2> Accessed on 2nd April 2020

[13] James Vincent, 'A rear example of AI fooling people in the wild'. Available at <https://www.theverge.com/2019/6/13/18677341/ai-generated-fake-faces-spy-linked-in-contacts-associated-press> Accessed on April 3rd 2020

/ networking platforms; (ii) the enhancement in the computing powers of graphics processing units (GPUs) and neural networks (an AI variant); and (iii) the growing commodification of tools and services that lower the barrier for non-experts to create deepfakes.[14]

Regardless of newer advancement in deepfakes, the major challenges often associated with the technology can be narrowed down as follows. Firstly, the challenge of anonymity denotes that majority of deepfake creators hide their identity, thereby making them untraceable to their victims or regulatory bodies. This problem is further compounded in cases where such creator is located in another jurisdiction.[15] Secondly is the reality that the internet has no borders with regards to the fast pace at which news, particularly misinformation spreads. The wrongful activities of individuals over deepfakes can have lasting effects on others, thereby leaving impressions which may be particularly difficult to correct afterwards. Another challenge is that deepfakes may be used by individuals to escape accountability for the truth. Situations occur whereby a person accused of a wrong, may use adapted videos or audio evidence to create doubt about the accusation or contradict the claim outrightly by regarding such authentic video or content as a deepfake. This is often referred to as the "liar's dividend'.[16] Lastly, is the concern that the technology is improving so fast that it will soon be much more difficult to distinguish a deepfake from the real thing.[17] This would ultimately result in people being generally skeptical about the veracity of every image or video they come across.

III. HOW ARE DEEPFAKES USED?

It is often said that *"a tool is only as good as the hands of the one who wields it"*[18]; same thing can be said of deepfakes. *Whilst deepfakes could be highly innovative with an inherent creative and commercial value,* there have been numerous attempts to create socially harmful deepfakes. The varied uses of the deepfake technology can be traced to the following creators including – i) deepfake hobbyists; ii) political and various activists; iii) other malevolent actors such as fraudsters; and iv) legitimate creators, such as e-commerce companies, movie production companies, educational and health institutes etc.

In discussing the forms of deepfakes, this work classifies the use of deepfake technology into two (2) broad categories – Criminal and Commercial uses.

Criminal Use of Deepfakes

a) The very first use case of GANs was to create deepfake sex videos; in particular, face-swapped celebrity porn and revenge porn. In the former category, celebrities' images are superimposed on the bodies of porn stars in adult movies. This kind of non-consensual celebrity pornography still

[14] Adam Green, 'Lawmakers and tech groups fight back against deepfakes', Financial Times (Oct 2019). Available at <https://www.ft.com/content/b7c78624-ca57-11e9-af46-b09e8bfe60c0>. Accessed on 3rd April 2020
[15] Holly Kathleen Hall, 'Deepfake Videos: When Seeing Isn't Believing', 27 Cath. U. J. L. & Tech 51 (2018). Available at: https://scholarship.law.edu/jlt/vol27/iss1/4. Accessed on April 2nd 2020
[16] Chesney & Citron (n 4)
[17] Nadine Krefetz, 'Deepfakes and the War on Reality'. Available at <https://www.streamingmedia.com/Articles/ReadArticle.aspx?ArticleID=139414>. Accessed on 31st March 2020
[18] Unknown origin

accounts for about majority of all the deepfakes.[19] On the other hand, revenge porn has been subsequently expanded to deepfake sex videos, where non-consensual pornographic deepfakes are distributed by hackers or anyone seeking financial gain or notoriety rather than merely as a revenge for the loss of a romantic relationship.[20]

Although, the earliest deepfake pornography featured such famous actresses as Scarlett Johannsson and Gal Gadot, however, the reality is that anyone could have his or her face superimposed onto the bodies of porn stars engaged in sexual acts. Hence deepfake sex videos raise issues of breach of privacy, violation of image rights (where applicable), and consent, often resulting in victims suffering sexual humiliation and exploitation; physical, mental or financial abuse, damage to reputation, to mention but a few.

b) Deepfakes may also be used as a catalyst by various political players, including political agitators, hacktivists, terrorists, and foreign state intelligence agencies in disinformation campaigns to manipulate public opinion and to erode trust in public institutions. The negative impacts of deepfake videos / news reports to democratic societies could extend to targeting the reputation of certain individuals (e.g. a deepfake video of a politician offering / receiving a bribe), portray false or fabricated events (a fake terrorist attack or kidnap), or impact such democratic processes as electoral campaigns (a deepfake of a presidential candidate giving a racist speech or a presidential candidate confessing complicity in a crime), or and to deepen polarization among social groups.[21] Also, if used by hostile governments, deepfakes could even pose threats to national security or impair international relations.[22]

While the foregoing examples of deepfakes possess the likelihood of causing domestic unrest, riots, and disruptions in elections, other nation states could even choose to act out their foreign policies based on unreality, leading to international conflicts.[23] The end result is that such deepfakes are likely to hamper citizens' trust toward authority-provided information and therefore come to regard everything as untrue.

c) Cybersecurity issues constitute one of the major threats imposed by deepfakes. The corporate world is gradually witnessing deepfakes being deployed by fraudsters to commit financial fraud. Criminals can make use of deepfake technology for market and stock manipulation; create real-time visual and audio impersonations of executives announcing a fake product launch, or fake acquisition / merger, making false statements of financial losses, bankruptcy or even the capabilities of a product, or portraying them as if committing a crime, or even giving instructions to an employee to perform an urgent cash transfer or provide confidential information; the list is

[19] Mesky, Liaudanskas et al (n 8)
[20] Ibid
[21] BJ Siekierski, 'Deep Fakes: What Can Be Done About Synthetic Audio and Video?'. Available at <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201911E> accessed on 31st May 2020
[22] Mesky, Liaudanskas et al (n 8)
[23] Carter Evans, 'Spotting Fakes News in a World with manipulated video' (CBS News, April 17, 2018). Available at <https://www.cbsnews.com/news/spotting-fake-news-in-a-world-with-manipulated-video/>. Accessed on 31st May 2020

endless.[24] As such, with the quality of these videos improving rapidly, businesses need to be aware of how to spot fake videos, if not they stand the risk of brand sabotage, blackmail, falsification of evidence against a business in court, embarrass management, subvert procurement process, disrupt business relationships and ultimately result in loss of business.

Commercial Use of Deepfakes

Deepfake technology also has positive uses in many industries, including entertainment, social media and healthcare, educational media and digital communications, and various business fields, such as e-commerce and fashion. Businesses in the e-commerce and advertising sector interested in brand distinction can adopt deepfake technology in transforming their products or services in significant ways thereby making same easily distinguishable by customers. For example, an e-fashion store may allow customers create digital clones / avatars of themselves and try on attires before final purchase.[25]

The movie industry can benefit from deepfake technology in several ways. Initially, movie studios faced diverse challenges in bringing the imaginations of creators (writers / directors) into reality owing to the limitations of technology, and where said technology was available, visual storytelling remained prohibitively expensive for most creators. However, deepfake tech incorporates the ability to merge imagery, thereby giving smaller-scale and up-coming producers a similar capacity for bringing imaginative creativity to life at a reduced cost.[26] Examples of use and potentials of deepfake in the movie industry include - updating film footage instead of reshooting it, recreation of classic scenes in movies, create new movies starring long-dead actors, make use of special effects and advanced face editing in post-production, rendition of digital voices for actors who lost theirs due to disease etc.[27]

Similarly, deepfake technology can break the language barrier on video conference calls by translating speech and simultaneously altering facial and mouth movements to improve eye-contact and make everyone appear to be speaking the same language.[28] This can be extended to creating realistic voice over or dubbing for movies in any language, thus allowing diverse audiences to better enjoy films and educational media. A good example is the 2019 global malaria awareness campaign featuring David Beckham wherein visual and voice-altering technology was used to make him appear multilingual.[29] In the same vein, deep fakes could be generated as a form

---

[24] Donie O'Sullivan, 'House Intel chair sounds alarm in Congress' first hearing on deepfake videos', Available at <https://edition.cnn.com/2019/06/13/tech/deepfake-congress-hearing/index.html> accessed on 31st May 2020

[25] Katie Baron, 'Digital Double: The Deepfake Tech Nourishing New Wave Retail', 29th July 2019 Available at < https://www.forbes.com/sites/katiebaron/2019/07/29/digital-do-ubles-the-deepfake-tech-nourishing-new-wave-retail/#33489a044cc7>. Accessed on 7th April 2020

[26] Sunny Dhillon, 'The optimistic view of deepfakes', 4th July 2019. Available at < https://techcrunch.com/2019/07/04/an-optimistic-view-of-deepfakes/> Accessed on 7th April 2020.

[27] John Brandon, *Terrifying High-Tech Porn: Creepy 'Deepfake' Videos Are on the Rise*, FOX NEWS (Feb. 16, 2018), http:// www.foxnews.com/tech/2018/02/16/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-rise.html

[28] Matt Ballantine, 'Are Deepfakes Invading the Office?', 3rd July 2019, Available at < https://www.forbes.com/sites/mattballantine/2019/07/03/are-deepfakes-invading-the-office/#19bf48923ea1> Accessed on 7th April 2020

[29] Available at <https://www.youtube.com/watch?v=U-mg7a1vwkw>. Accessed on 7th April 2020

of parody or satire (e.g. videos, memes, etc.). GANs certainly empower creators to create new content and develop innovative forms of creative expression. Accordingly, deep fakes could be seen as a medium that facilitates creative interactions and political debates. Creative deep fakes could be considered a constitutive part of free speech. The possibilities of deepfakes are endless and the true potentials yet to be fully exploited.

IV. LEGISLATION AND REGULATION OF DEEPFAKES

In view of the probable uses and misuses of deepfakes as discussed earlier in this article, the roles of legislation and regulation cannot be overemphasized. For legitimate commercial use, the presence of comprehensive legislation setting out a workable framework governing creation, ownership, distribution and responsible exploitation is required. In similar vein, in cases of criminal use, the enactment of new penal laws and/or regulations or the revision of extant ones capturing these realities hitherto not contemplated is desired.

Presently, deepfakes are not specifically mentioned by civil or criminal laws in Nigeria, however, a look at a few of the extant laws and regulations discloses the possibility of adapting such laws to address issues bordering on privacy & data protection, intellectual property, defamation, identity fraud, or impersonation from the use of deepfakes and further help in allowing the creators or users of deepfakes know what types of deepfakes are and are not permissible.

Data Protection and Privacy Laws

Nigeria's data protection and privacy regulatory framework stems from the fundamental right to privacy under Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as Amended). The breach to the privacy of individuals may generally be viewed as - an intrusion of personal life (with regards to how information was obtained); publicity given to private life; publicity in false light; and wrongful appropriation.[30] As such, a victim of deepfake may bring an action for breach of his constitutional right to privacy where such person can successfully persuade the court to construe the constitutional right to privacy as a right covering the intrusion of one's private life particularly with respect to how photographs or videos are obtained and subsequently deepfaked. However, despite the foregoing constitutional guarantee of the right to privacy, Nigerian jurisprudence on the point has remained largely undeveloped as other climes have moved forward to also make provisions for laws safeguarding issues on personality and image rights, to mention but a few.

Presently, Nigeria does not have any principal legislation on data protection, however, there exists a subsidiary data protection regulation: the Nigeria Data Protection Regulation 2019 (the "Regulation").[31]As an advancement on privacy rights, the primary aim of the Regulation is to protect the personal data of all Nigerians and non-Nigerian residents in Nigeria. Also, the Regulation applies to all transactions that involve the processing of personal data and sensitive

[30] Russell Spivak, "Deepfakes: The Newest Way to Commit One of the Oldest Crimes", 3 GEO. L. TECH. REV. 339 (2019), page 377

[31] Issued by the National Information Technology Development Agency (NITDA) on 25th January 2019. The said Regulation was made pursuant to the National Information Technology Development Agency Act (NITDA Act 2007).

personal data.[32] The term 'Personal data' is defined as 'any' information relating to an identified or identifiable natural person. Amongst other terms, personal information (sensitive or otherwise) includes names, photographs, and any other information specific to the physical, physiological, genetic, economic, cultural or social identity of that natural person.[33] The Regulation further defines the term 'Processing' to mean 'any' operation or set of operation which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[34]

A significant provision of the Regulation is the requirement that consent must be obtained by data controllers before processing the personal data of individuals or transferring such data to third parties.[35] As such, where a developer of a face-swapping mobile app inserts provisions in its terms and conditions giving the developers the global right to 'permanently' use any image created on the app for free or gives the developers the right to transfer this images to any third party without further permission from the user, this would clearly amount to a data breach under the Regulation.[36]

Deepfakes are by their nature captured under the Regulation, as they involve the process of **collection, recording, organisation, storage, adaption, alteration, retrieval, use, disclosure or dissemination** of personal information of individuals.[37]Hence, it is important that the appropriate consent be first sought and obtained in order not to be caught for data and privacy breaches, particularly where an organisation plans to use data for purposes that are not apparent to the individual. Also, in addition to the importance of obtaining consent before the processing of any personal data, the Regulation further provides for other permissible grounds where data may be processed without necessarily obtaining consent before such processing, as in the case of data processed for the performance of a contract to which the Data Subject is party or for compliance with a legal obligation to which the Controller is subject.[38] In placing reliance on foregoing grounds, legitimate creators such as e-commerce companies or movie production companies in the "performance of a contract to which the data subject is a party" may not be required to obtain 'consent' before processing such personal data.

Intellectual Property

Creating modified content as the case with deepfakes would generally raise issues bordering on intellectual property protection, particularly from the copyright perspective. Deepfakes raise

[32] Regulation 1.2 of the NITDA Data Protection Regulation
[33] Reg. 1.3 of the NITDA Data Protection Regulation
[34] Ibid
[35] Reg. 2.2 & 2.3 of the NITDA Data Protection Regulation
[36] In 2019, China face-swapping app "Zao" that uses selfies from the user's phone to convincingly change a character's face from clips of films and TV shows, sparked controversy about privacy and fraud concerns, particularly with regards to its end-use agreement which permitted unrestricted use and transfer by the company of images / clips created. < https://www.bbc.com/news/technology-49570418> Accessed on 11th April 2020
[37] Reg 1.3 defines what 'Processing' of personal data entails
[38] Reg. 2.2, lists the grounds for which data may be processed.

questions ranging from whether the creator of a deepfake could claim copyright authorship of the newly created deepfake or whether the use of the original content (one or multiple copyright works) without consent amounts to an infringement of third-party copyright and/or image rights, amongst other controversies.

Under Nigeria's primary Copyright legislation, to establish infringement, two elements must be proven: (i) ownership of a valid copyright, and (ii) copying of constituent elements of the work that are original. The ownership can be established by demonstrating that the claimant is the initial author, licensee or assignee of the work; but since the victims of deepfakes do not own the underlying copyright of the source material, victims ordinarily have no copyright claim.[39] Hence, it is only the author of the copyrighted source material from which the deepfake was created who has the exclusive rights to file a copyright infringement suit. For example, the copyrights in a photograph are vested in the person who took the photograph, i.e. the photographer, thereby giving such photographer and not the victim of a deepfake right to make a claim of infringement against a deepfake creator.[40]

In situations where the deepfake involves a photo that the victim took of himself, then such victim as author might have a copyright claim against the creator of the deepfake. However, the chances of success in such suits are uncertain, as creators of deepfakes may avoid liability by invoking statutory exceptions showing that the deepfake constitutes a "fair use" / "fair dealing" of the copyrighted material, intended for educational, artistic, or other expressive purposes as a parody or satire, or that only small portion of the original work was used to create deepfake (e.g. if only a short snippet of a film was used in creating a parody).[41]

The issue of whether a creator of a deepfake can escape liability will depend on the facts of each case, and more importantly whether the alleged infringer can persuade the court that the fair use analysis sets the balance in his/her favour, by showing that the deepfake is transformative in nature and that the deepfake is intended to be used for purposes other than commercial purposes.[42]Similarly, a victim may take steps in ensuring the infringing content is taken down by issuing a complaint to an Internet Service Provider (ISP) to take down an identified content (a takedown notice).[43]

Another avenue for recourse lies in asserting image rights / rights to publicity. Image rights (referred to as right of publicity in some jurisdiction like the US) is an intellectual property right which has been defined as the inherent right of every human being to control the commercial use of aspects of his personality, such as physical appearance, pictures, likeness or caricatures, computer generated images, signature, personal logos, slogans etc.[44] Plainly put, "the image right"

[39] Sections 6, 10, 15 & 16 of the Copyright Act, CAP C28, LFN, 2010
[40] Section 51 of the Copyright Act
[41] Second Schedule to the Copyright Act
[42] Chesney and Citron (n 4)
[43] The Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission (NCC), sets out a procedure by which ISPs are obligated to takedown an illegal content either at the instance of the NCC or a person whose interest is harmed by such content.
[44] See: Proactive Sports Management Ltd v. Wayne Rooney & Ors [2010] EWHC 1807 (QB)

is an economic right to use the value of one's own prominence.[45] Although initially associated with celebrities, professional athletics, artists and entertainers, images rights have gradually been expanded to include non-celebrities.[46]

A claim for breach of image rights could also be an avenue to address harm from deepfakes. As such, if a creator profits from using another person's image in a deepfake without that person's consent, the person whose likeness appears may be able to bring an image rights claim. All that a claimant must prove in an image rights suit is that he enjoys goodwill or considerable influence entitling him to a pecuniary interest in his identity, and that such identity has been commercially exploited by a defendant without consent.[47] Unlike copyrights actions, one benefit for victims bringing a claim for breach of their image rights, is that the right to bring the claim does not depend upon legal ownership of the image.[48]However, a defendant may again likely raise the defence that the work was for purely expressive purposes as a parody or satire, or that no commercial benefit was derived from the work.

Presently, there is no comprehensive law providing for image rights in Nigeria. Although, it has been suggested that image rights are covered by copyrights law in Nigeria as an extension of artistic works and cinematographic films and therefore eligible for copyright protection.[49] However, it is submitted that actions under the heads of the torts of 'passing-off' and 'defamation' may present a more viable option for pursuing image right claims arising from deepfakes in Nigeria and it is to these heads we now turn.

Tort of Defamation

The tort of Defamation provides remedies for disparaging statements and representations geared at damaging people's reputations.[50] Under Nigerian law, variants of defamation consists of the twin torts of libel and slander. The former involves the publication of defamatory matter expressed in permanent form such as by writing, sign, picture, cartoon or electronic broadcast; while the latter category is restricted to utterances or spoken words. Since deepfakes are often expressed in permanent form, victims of deepfakes may be entitled to recovery under a defamation action within the purview of libel.

Defamation through online use and spreading false statements through web content with the aim of harming the target's reputation has become a problem in the age of the computer. This specie

[45] Spivak (n 18) page 383

[46] Prince-Alex Iwu, "Photo Privacy and Media / Image Rights in Nigeria", The BarCode 2017. Available < http://barcode.stillwaterslaw.com/1.1/2017/04/01/photo-privacy-and-mediaimage-rights-in-nigeria/>. Accessed 21st April 2020.

[47] Ibid

[48] Elizabeth Caldera, "Reject the Evidence of Your Eyes and Ears: Deepfakes and the Law of Virtual Replicants", Selton Hall Law Review 177, 2019, page 7.

[49] Davidson Oturu, "Nigeria: Protection of Image Rights (Part 1), Mondaq 29th October 2019. Available at <https://www.mondaq.com/Nigeria/Intellectual-Property/858520/Protection-Of-Image-Rights-Part-1>. Accessed on 21st April 2020

[50] Dr. Ayodeji Araromi, "Determining Legal Responsibilities in Defamation: Crossing the Dividing Line Between Real World and Internet Jurisdiction", Available at < https://www.researchgate.net/scientific-contributions/2075535661_Marcus_Araromi>. Accessed on 20th April 2020

of defamation could cover a wider range of locations and areas of the country or world than a usual defamation claim. Since deepfakes are majorly disseminated across the internet and other electronic means, the effect and description of the generic defamation essentially tallies with online defamation.[51] As such, for a case of an online defamation to become actionable the following conditions must be met – (i) the online defamatory statement must be a lie; (ii) there must be serious harm occasioned to the victim as a result of the statement; and (iii) there must be evidence of the publication.[52] For example, an individual who spends a lifetime cultivating a given reputation only to have it obliterated by a fraudulent adult video depicting false sexual actions, which he or she appears to partake in, when those actions run contrary to said reputation, likely has a cause of action that satisfies the standard for a defamation suit.

In relation to online defamation, in the context of a deepfake claim, a claimant must prove that - there was a substantial and real publication (i.e. the defamatory material was actually accessed and downloaded by identifiable persons within the jurisdiction of the court) of the alleged defamatory material and that reputational damage was suffered. However, in measuring reputational damage suffered by the victim of an online defamatory claim, recourse must be had to the readership of the defamatory material. The more the number of readers of the offending post, the greater the likelihood of reputational damage. Conversely, if the level of readership is low then a defamatory claim may very well fail unless it can be established on evidence that the posting has caused or is likely to cause serious reputational harm.[53]

It must be emphasized that not every 'negative' publication made online amounts to defamation. A defendant to a defamatory claim arising from deepfake creations may rely on the defence of – fair comment, statements of opinion arrived at based on facts; statements about public officials / figures, except there is clear and convincing evidence of actual malice by the creator of deepfake, this defence cannot be successfully raised; and where it is proven that the communication was the truth.

Competition Law

Unfair competition or business practice usually occurs through false information about a company, or advertising that draws attention away from a business or attracting the customers of a specific entity to the other. Unfair business practices encompass fraud, misrepresentation (inclusive of false advertisement), and oppressive or unconscionable acts or practices by businesses, often against competing businesses or consumers and are prohibited by law in many countries. The law of unfair competition may simply be referred to as any trade practice whose harm outweighs its benefits.[54]

---

[51] A. Atake SAN, E. Gbahabo et al, "Online Defamation: Just before You Post It!", Templars-Thought Leadership, 3rd April, 2019. Available at < https://www.templars-law.com/copyrights-and-the-music-business/>, accessed on 20th April 2020

[52] See: Wilson v. Bauer Media Pty Ltd (2017) VSC 521 (Australia), Giwa v. Ajayi (1993) 5 NWLR (Pt. 294) 423 5 and Omo-Agege v. Oghojafor (2011) 3 NWLR (Pt. 1234) at 341

[53] See: Mohammed Hussein Al Amoudi v. Jean Charles Brisard & Anor (2006) 3 All ER 294, and Monroe v. Hopkins [2017] EWHC 433 (QB)

[54] Lanre Adedeji, "Consumer Law and Unfair Business Practices", Available at < https://www.thelawyerschronicle.com/consumer-law-and-unfair-business-practices/>. Accessed on 22nd April 2020

In relation to deepfakes, unfair competition law may be brought in to curtail deceptive acts or practices which affects commerce and business. The technology behind the creation of deepfakes involves utilizing an individual's data and modifying it onto someone else's or creating something entirely different, and as such, where such modified data (video, photograph or audio) is utilized without consent in false advertisement of a commercial offering, or to misrepresent the goods of a competing business or to depict a false endorsement of a product / service, then such activity would fall within the purview of unfair or deceptive acts or practices in or affecting commerce.[55]

The current regime on competition in Nigeria is governed by the "Federal Competition and Consumer Protection Act 2018" (the "FCCPA"). The key objectives of the FCCPA amongst others include the protection of consumer interests and welfare, and prohibiting restrictive and unfair business practices in Nigeria.[56] The FCCPA further establishes the Federal Competition and Consumer Protection Commission (the "FCCPC"), which acts as the competition regulator empowered to prevent and punish anti-competitive practices in every sector in Nigeria.[57]

The unique powers of the FCCPC in developing rules and regulations governing consumer protection and competition protection make it a potential option for regulating deepfakes in Nigeria. However, the powers of the FCCPC may be limited as not every deepfake creation entails a 'commercial' component. As such, where a deepfake pornography or video is created for sexual gratification, or to humiliate a victim, or for other non-commercial purposes as a parody for entertainment purposes, then the FCCPC's regulatory jurisdiction in addressing such deepfakes would most likely be limited.

Criminal Sanctions

A number of current criminal statutes in Nigeria concerning cyber stalking, blackmail, extortion, impersonation, and criminal defamation are potentially relevant in addressing concerns arising from the criminal activities associated with deepfakes. The Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 remains at the forefront in tackling criminal activities bordering on the cyber space. Section 24 of the Cybercrimes Act criminalizes any intentional dissemination of a message or other matter by means of computer systems or network that - *is grossly offensive, pornographic or of an indecent, obscene or menacing character* which such person knows to be false, for the purpose of causing *annoyance, inconvenience danger, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another.* Hence, the posting of deepfakes in connection with the targeting of individuals, for example, where non-consensual pornographic deepfakes are shared would be in violation of the provisions of the said Sections 24.[58]

Again Sections 13, 14 & 22 of the Cybercrimes Act when collectively read, criminalizes activities relating to impersonation crimes (computer related forgery, fraud and identity theft), particularly where a person knowingly accesses any computer or network and *inputs, alters*, deletes or

[55] Spivak (n 30)
[56] Section 1 FCCPA
[57] Sections 3 & 17 (g) FCCPA
[58] Section 58 of the Cybercrimes Act defines "Computer Systems" as any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated or interactive processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones.

suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic, or where such actions (alteration, inputs) causes any loss of property to another, whether or not for the purpose of conferring any economic benefits on himself or another person. The offence also covers instances where a person sends electronic message materially misrepresents any fact with an intent to defraud another.

It follows that where a deepfake video is created and circulated for the purpose of causing *"annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety"* to another, or where such video is used to perpetuate fraud, then the relevant provisions of the Cybercrime Act may be applicable in penalizing such actions.[59]In addressing the harms that may be of a broader nature with respect to the society at large, Section 26 of the Cybercrimes Act criminalizes activities involving the creation or distribution of racist or xenophobic materials to the public through a computer system or network. So, a deepfake containing a racist or hate speech is circulated to incite / spur an audience to violence would be captured under this provision of the Cybercrimes Act.

Creators of deep fakes could also face charges for criminal defamation if they posted videos knowing that they were fake or if they were reckless as to their truth or falsity. Unlike the tort of defamation as discussed in the earlier part of this work, in criminal defamation, the law seeks to prevent a situation in which defamation assumes a tendency to arouse angry passion, provoke revenge and set the society ablaze in a way that public peace is endangered.[60]

Section 373 of the Criminal Code defines defamation as a matter likely to injure the reputation of any person by exposing him to hatred, contempt or ridicule, or likely to damage any person in his profession or trade by injury to his reputation. As with the tort of defamation, such defamatory matter may be referred to as slander if expressed / published in a transient. While a more permanent publication, either printed or written, of a false and injurious material against another person, whether it be in painting or picture, effigy, caricature, advertisement, article, news report, talking film or any disparaging object will qualify as libel.

Publication again remains a vital element in criminal defamation. Whereas in tort the false publication must be to a third party before it is taken as defamatory, in the crime of defamation, however, publication to the person defamed alone is enough.[61] Hence an indictment will lie in Criminal Libel where the libel falsely published and tends to provoke the person defamed to commit a breach of the peace.[62]

[59] Sections 13, 14 & 22 of the Cybercrimes (Prohibition, Prevention Etc.) Act 2015, and other sections therein imposes fines and / or a term of imprisonment as penalties for violations of the Act.
[60]Afe Babalola SAN, "When False Publication May Amount to Criminal Libel", Available at < http://www.abuad.edu.ng/when-false-publications-may-amount-to-criminal-libel/>. Accessed on 25th April, 2020.
[61] Section 374 of the Criminal Code
[62] Babalola, SAN (n 60)

Other Methods of Combating Deepfakes

It must be emphasized that in addition to the use of regulation in addressing concerns arising from deepfakes, there are other approaches that may be used in combating the harm caused by deepfakes. These combative approaches are:

a. Corporate policies and voluntary actions – This would include the creation of policies by social media firms to report, block or remove deepfake content; suspending user accounts of violators; investing in detection technologies; train staff to identify deepfakes etc.[63]

b. Development of technology for deepfake detection, content authentication, and deepfake prevention. This provides numerous business opportunities for technology entrepreneurs in the field of cybersecurity and AI.[64]

c. Education and training: The threat of deepfakes has not yet been reckoned with by the public. There is a need to raise public awareness about the technology's potential for misuse. Also, companies and organizations, in addition to training staff members, need to be on high alert and to establish cyber resilience plans. E.g. having a thorough verification strategy / system; or the use of slogans and codes known only to staff or team members.[65]

V. CONCLUSION

As a new technological process creating new possibilities, deepfakes are here to stay, and that is beyond doubt. Although the criminal uses of deepfakes are unavoidable, such inevitability should not displace the need to recognize the huge commercial potentials of the technology, nor should same preclude attempts to impede or mitigate the potential harms that the technology is likely to cause.

More often than not, the gap between emerging novel technologies, such as deepfakes, and the systems set up to regulate them have only grown broader. The systems are often non-responsive and slow to respond/adapt to the rapid changing societal and economic circumstances introduced by these emerging technologies. Also, these regulatory challenges are further compounded by the existing complex national systems in place for enacting new laws, or modifying old ones to respond to recent and/or emerging developments. The current regulatory framework in Nigeria is no exception, as it lacks a mechanism that succinctly and anticipatorily informs law makers of beneficial innovative technologies.

In spite of the absence of any full-blown report of the use of deepfakes in Nigeria nor the express mention of the term "deepfakes" in our legal jurisprudence, this article demonstrates, that some of

[63] Oscar Schwartz, 'Deepfakes aren't a tech problem, they are a power problem'. Available at < https://www.theguardian.com/commentisfree/2019/jun/24/deepfakes-facebook-silicon-valley-responsibility> Accessed on 4th June 2020

[64] Westerlund (n 6). See also: Drew Hawell, 'Top AI researchers race to detect 'deepfake' videos: 'We are outgunned', Available at <https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/> Accessed on 4th June 2020

[65] Kalev Leetaru, 'Deepfakes: The Media Talks Politics While the Public is Interested in Pornography'. Available at < https://www.forbes.com/sites/kalevleetaru/2019/03/16/deepfakes-the-media-talks-politics-while-the-public-is-interested-in-pornography/#71ea2e528461> Accessed on 4th June 2020

our pre-existing laws spanning Intellectual Property, Data Protection, Privacy, Competition law, Torts and Criminal statutes to mention but a few, may be adopted as initial approaches in addressing concerns arising from deepfakes. However, the need for the repealing and / or amendment of our existing legislations to cure latent ambiguities that may arise with regards to the applicability of those rules to deepfakes and other emerging technologies cannot be over emphasized, as it is the rate at which the law is clarified or amended to overcome such hurdles that may be viewed as its pace of 'adaptation'. This process will of necessity involve adopting measures that are built on flexible and inclusive processes that involve innovators, startups and established companies, regulators, experts and the public in the law-making/review process.

Consequently, in addition to updating the existing laws and regulations, there must be in place a well-defined strategy having a combination of educational, legal/regulatory and sociotechnical approach to the deepfake technology, because once the rubber hits the road, no one would be immune.