American Journal of
Leadership and Governance
(AJLG)

An Appraisal of the Implications of Deep Fakes: The Need for Urgent International Legislations

Nmesoma Nnamdi, Dr. O.A. Oniyinde & Dr. B. Abegunde

AJP

American Journal of Leadership and Governance
ISSN 2957-7284 (Online)
Vol.8, Issue 1, pp 43 – 70, 2023
www.ajpojournals.org

An Appraisal of the Implications of Deep Fakes: The Need for Urgent International Legislations

Nmesoma Nnamdi[1*], Dr. O.A. Oniyinde[2] and Dr. B. Abegunde[3]
[1]LL.B Hons, B.L (in view), High Court of Justice, Ado –Ekiti
[*]Corresponding Author's Email: nmesomannamdi1@gmail.com
[2]Ph.D, Reader, Faculty of Law, Ekiti State University, Ado Ekiti
Email: iyinlade@yahoo.com
[3]Ph.D, Reader, Faculty of Law, Ekiti State University, Ado Ekiti
Email: babalola.abegunde@eksu.edu.ng

Article History
Received: 02. 07.2023, Received in revised form: 22.07.2023, Accepted: 23.07.2023

Abstract

Purpose: Artificial intelligence as a subfield of the Fourth Industrial Revolution has been a controversial concept since its inception. The reason for its controversy is that through it, incredible inventions and also inventions detrimental to the society have surfaced. A deep fake is an Artificial Intelligence technology that creates videos and images of persons and events that in fact did not happen. The aim of this paper is to evaluate the concept of deepfake, its positive impacts and threats posed to individuals, corporate institutions and nations. It further assesses the legal implications of and provisions against deep fakes.

Methodology: The research methodology adopted in this study is doctrinal. Just like every Artificial Intelligence technology, it has benefits that cut across the marketing, fashion, and art industry among others. However, the issue for determination remains whether the positive impact of this AI technology supersedes the negative impacts.

Findings: Findings revealed that it has a high tendency to deceive an average person and also create uncertainty about the authenticity of a piece of information. This can lead to the spread of fake news, fraud, blackmail, fabrication of evidence, and even national and global insecurity. Trust in the social media and the internet generally will face a great decline at the spread of deepfakes, this will then be a medium for denial of videos that are in fact true.

Unique Contribution to Theory, Practice and Policy: The world is set to face a new and modified aspect of social engineering that will require an upgrade in cybersecurity techniques and strategies. By virtue of the sensitivity of the negative impacts of deepfake, this study concludes that it is necessary to promulgate legislations both at national and international levels to curb or regulate deepfakes.

Keywords: *Deepfake, Artificial Intelligence, Impacts, Laws, Regulations*

American Journal of Leadership and Governance
ISSN 2957-7284 (Online)
Vol.8, Issue 1, pp 43 – 70, 2023
www.ajpojournals.org

1.0 INTRODUCTION

The advent and escalation of Artificial Intelligence, which is the most famous sub-field of the Fourth Industrial Revolution, has introduced novel crimes in society and cyberspace especially. Deep fakes are recent developments via AI that have stormed and taken over the internet. Deep fake, via a form of Artificial Intelligence called deep learning, makes images of fake events, hence the name "deep fake".[1]

The research methodology adopted in this study is the doctrinal legal research methodology. Primary reference is drawn from regulations and statutes, explaining their contents in relation to the subject matter, and identifying the lacuna therein. Data is also collected from journal articles and online materials relating to the subject matter.

A deep fake is a type of Artificial Intelligence used to create convincing images, audio and video hoaxes.[2] Simply put, it is a video or sound recording that replaces someone's face or voice with that of someone else, in a way that they appear real.[3]Deep fake is not the same as photoshop. Photoshops are tacky face swapping images that can be easily detected. Faceswaps via photoshops are usually disproportionate, uneven and do not match, however, deep fakes are hyper-realistic. The first versions of deep fakes shared the same tacky attributes as photoshops, but they have evolved to a nearly undetectable stage. Deep fakes are absolutely fictitious, yet are believable. Deep fakes could be exerted on the face, voice, and even motion of a person.

Deep fake was born in 2017 when a Reddit user posted doctored porn clips on the site. The user with the name "Deepfake" swapped the faces of celebrities like Gal Gadot, Taylor Swift, Scarlett Johansson and other prominent female actresses on porn performers.[4]Currently. Deep fakes are now accessible, that is, they can be created by anyone without technicalities as deep fake software applications have surfaced. This accessibility and anonymity has made its malicious use multiply, as anyone can create malicious videos of anyone, mostly celebrities and politicians, and still remain anonymous.

There are thousands of deep fake videos and pictures on the internet, some of which are easy to detect because of their poor quality,[5] while some are very believable and convincing that a reasonable with average intelligence would deem it real. Several videos like Mark Zuckerberg's claim of "having total control of billions of people's stolen data", Barack Obama calling Donald Trump a "complete dipshit", Donald Trump's tape of boasting about grabbing women's genitals are all deepfakes, but very believable that some persons till date refuse to disbelieve it.[6] The internet was exposed to the huge risk of deep fakes when nearly £200,000 from a UK subsidiary

[1] Ian Sample. (2020, January 13). *What are Deepfakes and how can you Spot them?*The Guardian.Retrieved May 8, 2023 from https://amp.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them
[2] Nick Barney. (n.d.). *Deep Fake AI (deepfake)*. Techtarget. Retrieved May 8, 2023, fromhttps://www.techtarget.com/whatis/definition/deepfake
[3] Cambridge Dictionary. (n.d.).*Deepfake*. Retrieved May 8, 2023, from https://dictionary.cambridge.org/dictionary/english/deepfake.
[4] Ian Sample, (supra).
[5] A deep fake video, when poorly or averagely made, can be easily detected via bad lip synching, patchy skin tone, or even flickering around the edges of transposed faces, or the teeth.
[6] Ian Sample, (supra).

of a German firm was paid into a Hungarian bank account in March 2019, upon belief that the instruction was made by the German CEO, whose voice was in fact deepfaked.[7]

Mike is of the view that there are at least four major types of deep fake producers namely, (i) Communities of deep fake hobbyists; (ii) political players such as foreign governments and various activist; (iii) other malevolent actors such as fraudsters and (iv) legitimate actors, such as television companies and community consists of both persons who use deepfake for fun (absence of threat and trickery) and those who do not.[8] Hobbyists indulge in deep fakes primarily for humor. They rarely have the intent to trick or threaten as they use the AI crafted memes and videos to attract followers to their social media pages. On the other hand, deepfakes are employed by activists or hacktivists to facilitate an agenda to manipulate public opinion.It can also be used to manipulate election results thereby creating unrest. As a matter of fact, the opposition government in a bid to bring down the ruling party in the eyes of the citizens, can employ deep fakes to blackmail them. In the finance and marketing industry, deepfakes can be used to manipulate figures and stock manipulation. It has been stated that in subsequent times, video calls will also be able to be faked in real time.[9]

Statement of the Problem

Undoubtedly, deep fakes contribute positively to society, however, it has become a regular tool used by malicious actors to disseminate false information. Deep fakes are capable of disrupting and diverting justice. It can be used by either parties to a suit to claim alibi, by making realistic videos of themselves in places and events that they never really were. It can lead to lack of trust in the media, hence, giving room for negative occurrences. When nobody believes what is said in the media or deems them to be false, this implies that true information will also be disregarded. It is noteworthy that the society thrives on trust, and security is built on trust, therefore, where this is lacking, insecurity will creep in. Deep fakes can also be used as a social engineering scheme to extort money from people. Upon evaluation of the numerous negative uses of deep fakes, which are already ongoing, it is crucial to establish specific international and national legislations that will address these issues and control the use of deep fakes. Furthermore, it is also necessary to set up institutions that will oversee the implementation and compliance with the legislation.

2.0 How Deep Fakes are Made

Deep fakes are a result of the applications that merge, combine, replace, and superimpose images and video clips to create fake videos that appear authentic.[10]Deep fakes are the product of Generative Adversarial Networks (GANs) and Artificial Neural Networks working together to create real-looking media. These two networks called “the generator”, and “the discriminator are trained on the same dataset of images, videos, or sounds. The first then tries to create new samples

[7] Ian Sample, (supra).

[8] Mike Westerland. (2019). The Emergence of Deepfake Technology: A Review. *Technology Information Management Review(9)(11),*39-52.

[9] O. Gonzalez. (2019, June 25).*Instagram Chief Adam Mosseri: We don’t have a Policy against Deepfakes*.*CNET*.Retrieved May 5, 2023, from https://www.cnet.com/google-amp/news/instagram-chief-adam-mosseri-we-dont-have-a-policy-against-deepfakes/.

[10] M. Maras and A. Alexandrou. (2019). Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos. *International Journal of Evidence and Proof (23)(3)*. 255-262. DOI: 10.1177/1365712718807226

that are good enough to trick the second network, which works to determine whether the new media it sees is real that way they drive each other to improve.[11]

These videos are so skillfully made with sophisticated devices and applications that they become hard to ascertain its authenticity.[12]It originates from deep learning algorithms which teach themselves to solve problems with large set of data and can be used to fake content of real people. Deep fakes are executed through neural networks which via large set analysis of data samples, learn to mimic a person's facial expressions, mannerisms, voice and inflictions.[13] A deep algorithm is fed with a footage of two different persons and the trained to swap faces.[14]

To create a realistic deepfake that is, one that is convincing to a reasonable man of average intelligence, numerous images are required in the processes, however, researchers have invented a novel technique to generate a realistic video by feeding it only one photo.[15]As a matter of fact, it has been stated that GANs, in the nearest future will be trained on less information and be able to swipe heads, whole bodies, and voices.[16]

[11] R. Metz. (2019, June 12).*The Fight to Stay ahead of Deepfake before the 2020 US Election*.*CBN*.Retrieved May 6, 2023, fromhttps://www.amp.cnn.com/cnn/2019/06/12/tech/deepfake-2020-detection/index.html; T. Chivers. (2019, June 23).*What do we do about Deepfake Video?*The Guardian. Retrieved May 6, 2023, fromhttps://amp.guardian.com/technology/2019/jun/23/what-do-we-do-about-deepfake-video-ai-facebook; M. Kan. (2018, September 17). *U.S. Lawmakers: AI Generated Fake Videos may be a Security Threat*. PC Magazine. Retrieved May 6, 2023, from https://ww.pcmag.com/news/us-lawmakers-ai-generated-fake-videos-may-be-a-security-threat.

[12] J. Fletcher. (2018). Deepfakes Artificial Intelligence and some kind of Dystopia: The New Faces of Online Post-Fact Performance.*Theatre Journal 70 (4)*, 455-471. DOI: 10.1353/tj.2018.0097.

[13] Mike Westerland, (supra)

[14] M. Eddy and N. Rubenking. (2019, August 9). *Detecting Deep Fakes may Mean Reading Lips*. PCM Magazine.Retrieved May 6, 2023, fromhttps://ww.pcmag.com/news/detecting-deepfakes-may-mean-reading-lips

[15] C. Evans. (2018, April 17). *Spotting Fake News in a World with Manipulated Videos.*CBS News. Retrieved May 6, 2023, from https://www.cbsnews.com/amp/news/spotting-fake-news-in-a-world-with-manipulated-video/; J.E. Solsman. (2019, May 24).*Samsung Deepfake AI could Fabricate a Video of you from a Single Profile Picture*.CNET.Retrieved May 6, 2023, fromhttps://www.cnet.com.com/google-amp/news/samsung-ai-deepfake-can-fabricate-a-video-of-you-from-a-single-photo-mona-lisa-cheapfake-dumbfake/..

[16] A. Hern. (2018, March 12). *My May-Thatcher Deepfake won't Fool you but its Tech may change the World.*The GuardianRetrieved May 6, 2023, fromhttps://amp.theguardina.com/technology/2018/mar/12/may-thatcher-deepfake-face-swap-tech-change-world; J. Andrews. (2019, July 12). *Fake News is Reality – A.I. is going to make it much Worse?* USA Today. Retrieved May 6, 2023, from https://www.cnbc.com/amp/2019/07/12/fake-news-is-real-ai-is-going-to-make-it-much-worse.html;Mike Westerland, (supra).

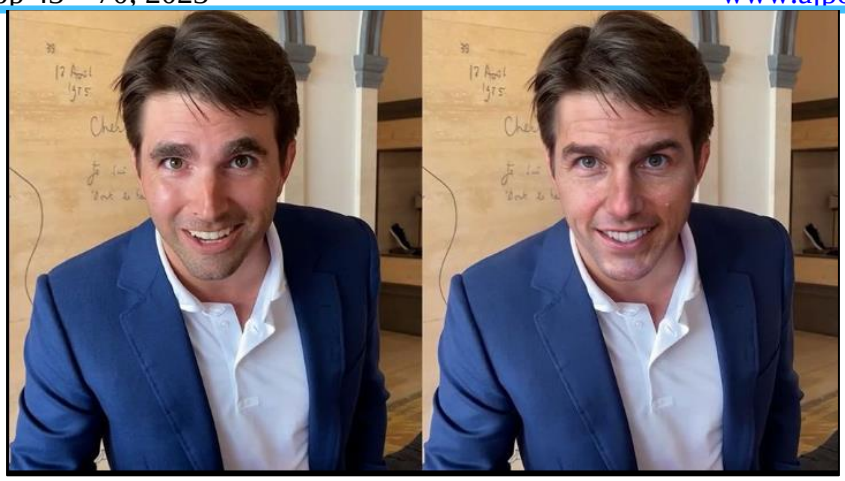

Figure 1: A Sample of a Man Hyper-Realistically Deepfaked into Hollywood Actor, Tom Cruise.[17]

3.0 FINDINGS

An Analysis of the Positive Impact of Deepfakes

Deep fakes are not always used for malicious intent. They can be used to restore people's voices when they lose them to diseases, and can enliven galleries and museum. In Florida, the Dali museum has a deepfake of the surrealist painter who introduces his art.[18]Deepfake offers a multi-lingual advantage. For instance, a visual and voice altering technology used in a 2019 global malaria award campaign featuring David Beckham, made him appear multi-lingual and reach out to a vast audience.[19]Deep fake can digitally bring a deceased loved one back to life. For instance, Deep Nostalgia allows users to add live motion to a still image of an ancestor or historical video. They take samples of humans moving their faces and apply it to the picture (in motion). This warms the heart of the people.It also helps people with Alzheimer's interact with a younger face they remember.It has been proposed that GANs can be used to detect abnormalities in X-rays as their protection in creating virtual chemical molecules to speed materials, science and medical recoveries.[20]

It can also be used in the fashion industry to aid customers clone themselves and know which clothes fit even without trying it on. In the fashion industry, through AI powered hyper-personalisation, many companies can now develop virtual fitting rooms where customers can scan their body and 'try on' the clothes before making purchases online. In addition to that, deep fakes can allow customers to try out the latest clothing in the virtual space. Data Grid, a Japanese AI

[17]Biance Britton. (2021, March 5). *Deepfake Videos of Tom Cruise went Viral. Their Creator Hopes they Boost Awareness.*NBC News.Retrieved May 17, 2023, from https://www.nbcnews.com/tech/tech-news/creator-viral-tom-cruise-deepfakes-speaks-rcna356

[18] Ian Sample, (supra).

[19] J. Brandon. (2018, February 16).*Terrifying High-Tech Porn Creepy "Deepfake" Videos are on the Rise.*Fox News. Retrieved May 8, 2023, fromhttps://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise

[20] T. Chivers, (supra); B. Dickson. (2018, June 7). *When AI Blurs the Line between Reality and Fiction.*PC Magazine.Retrieved May 8, 2023, from https://www.pcmag.com/news/when-ai-blurs-the-line-between-reality-and-fiction.

firm, allows customers to deepfake their faces onto their virtual models to see if those clothes fit or not. It helps especially in online shopping.[21]

Deep fake videos can convey an immersive marketing experience for a target audience through storytelling. Deep fake technologies allowed a voice synthesized John F. Kennedy to read a speech he never got to make. In the marketing industry, it can reduce the cost of video campaigns and provide hyper-personalised experience for customers.Instead of using an in-person actor, a marketer can purchase a license for an actor is identity. With previous digital recordings of the actor and inserted appropriate dialogue from a script for the actor, a new video can be created. As a matter of fact, where a person needed for an ad is busy, few previous recordings can be adopted to make an ad campaign. Voice synthesis can be used to create new dialogue to create a podcast, radio, or streaming services ad.[22]

In the film industry, instead of using traditional VFX for face-swapping which is time consuming and involves a lot of technicians, deepfake technology which only requires a couple of persons can be employed. Hence, only videos and images are required to be inputted, and Artificial Intelligence will swap faces, and replace such images in every frame.[23] Furthermore, deepfakes resolution can get to 1024 x 1024 which is a very huge improvement from 256 x 256 pixels making it more realistic and better on larger screen.

In journalism and media, human rights activists and journalists can use synthetic media to remain anonymous in dictatorial and oppressive regimes. Technology can be used to report atrocities. It can be used to mask the identity of people's voices and faces to protect their privacy.[24]

An Examination of the Threats and Negative Impacts of Deepfake

Deep fake is being used primarily in the negative, and unfortunately deepfake videos of false events have spread across the internet. Over 15,000 deepfakes videos were discovered online in September 2019 by an Artificial Intelligence firm called 'Deeptrace'. An evaluation of these vidoes revealed that 96% of them were pornography, and 99% of the fakes were female celebrities.[25]This result led persons like Danile Citron, a Professor of Law at Boston University to state that "deep fake technology is being weaponized against women."

Deep fakes are capable of intimidating, harassing, manipulating and blackmailing individuals, but beyond that, they are capable of inciting wars. For instance, a doctored video of troops crossing a nation's border or of a spy in another country can spark wars. Furthermore, it is not subject to doubt that deepfake is destroying trust in news by portraying believable fake news and fake events, and creating situations where people can no longer differentiate the truth from falsehood.

[21] Millie Chow. (2022, June 9). *What are the Positive Applications of Deepfake?* Jumpstart Magazine. Retrieved May 14, 2023, from https://www.jumpstartmag.com/what-are-the-positive-applications-of-deepfakes/; Eliot Ferrier. (2022, 24 June). *The Pros and Cons of Deepfake Technology Google News gets a redesign Tiktok's Platform Strategy Revealed, and Instagram's Main Feed to be revamped.* Intelligence.Retrieved May 14, 2023, from https://www.intelligencygroup.com/blog/digital-roundup-24-6-22.

[22] B. Dickson, (supra).

[23] Ibid.

[24] Ibid

[25] J. Berkowitz. (2019, October 7).*There are almost 15k Deepfake Videos out there- and 96% of them are porn.* Facts Company. Retrieved May 14, 2023, from https://www.fastcompany.com/90414116/there-are-almost-15k-deepfake-videos-out-there-and-96-of-them-are-porn

Deepfakes are also creating an avenue of denial of true events. Since deepfakes have become hyper-realistic that a reasonable person of average intelligence will deem them to be true, a person can also, through this medium, deny a true video simply because it is inconvenient or might not represent him well. Professor Lilian Edward, a leading expert in international law at Newcastle University believes that this is another negative aspect of deepfakes that must be looked into. According to her, "the problem may not be so much the faked reality as the fact that reality become plausibly deniable."[26] Henry Farid, a scholar at UC-Berkeley affirms Professor Edwards' statement where he states that "when anything can be fake, then nothing has to be real, and anyone can easily dismiss inconvenient facts." Furthermore, Henry Adjer, head of Threat Department at Deep trace, a Deep fake detection organization, warns that "the world is becoming increasingly more synthetic. [And Deepfake] is not going away.'[27] O'Sullivan and Patterson are of the view that the constant contact with misinformation is the most damaging aspect of deepfakes rather than disinformation, which is capable of leading people to feel that much information including videos simply cannot be trusted, thereby resulting in a phenomenon termed as 'information apocalypse' or 'reality apathy'.[28]

Deep fake also poses a great challenge to the legal system. Fake videos and pictures could be admitted as evidence since they are highly convincing, and what may be required by a person to disprove such might not be available to an average person. Subjecting the video to deep fake detection might be costly since it is not yet accessible, and requesting the service of a professional to detect the deepfake will also cost much. This can be easily admitted as evidence where there is no strong proof of alibi. Furthermore, the ability to deny true videos under the pretext of deep fakes makes it even harder to detect whether a person is lying or not. Deep fake can also be used as a strategy to prove fake alibi and incriminate parties in child custody battles, thatis present pictures or videos of a potential parent who might likely be granted custody, drinking or indulging in acts that could deprive such parent of custody.

Deep fakes, in the hands of bad actors, have been used maliciously, as in the case of New York High School students who made a deep fake of a Principal threatening Black students.[29] The main aim of malicious deep fakes should be addressed, which is that the maker of the photo or video had the sole aim of convincing people that the video or photo is real, when in fact, it is not.

Tech experts and academic writers like like Anlen and Lopez are of the view that the best approach the public can take to deepfake is to be informed about the technologies and its capabilities, rather

[26] Newcastle University. (2019, 14 June). *Newcastle Expert to Explore the Rise of Deepfakes*. Retrieved May 17, 2023, fromhttps://www.ncl.ac.uk/press/articles/archive/2019/06/deepfakrsbarbicantalk/

[27] Greg Noone. (2021, July 12). *How to Win the War on Deepfakes*. Retrieved May 17, 2023, from https://techmonitor.ai/technology/ai-and-automation/how-to-win-the-war-on-deepfakes-detecting

[28] D. O'Sullivan. (2019, August 10). *The Democratic Party Deepfaked its own Chairman to Highlight 2020 Concerns.*CNN. Retrieved May 17, 2023, from https://amp.cnn.com/cnn/2019/08/09/tech/deefake-tom-perez-dnc-defcon/index.html; D. Patterson. (2019, June 13). *From Deepfake to "Cheap Fake," it's Getting Harder to tell what's true on your Favorite Apps and Websites.*CBN News.Retrieved May 17, 2023, from https://www.cbsnews.com/amp/news/what-are-deepfakes-how-to-tell-if-video-is-fake/.

[29] David Gilbert. (2023, March 8). *High Schoolers made a Racist Deep Fake of a Principal Threatening Black Students.*Vice.Retrieved May 2, 2023, fromhttps://www.vice.com/enarticle/7kX2R9/school-principal-deepfake-racist-video

than panic.[30]There are several ways to detect a deepfake of low quality. They include, blurry details, unnatural lighting (since, the algorithms retain the lightening of the dual clips, it will definitely not match) lips matching with words, and background sound among others. However, with the upgrade in deepfake, detection via the mentioned way has become harder. As a matter of fact, Hao Li, a deepfake pioneer and Associate Professor has expressed that deepfake is developing more rapidly and "soon, it's going to get to the point where there is no way that we can actually detect (deepfakes) anymore, so we have to look at other types of solution."

Initially, one huge problem faced with social media was dissemination of fake news. However, as they were just mere written statements, people began to ignore messages until confirmation from trusted sources. However, the advent of deepfake has worsened the situation. With pictures and videos confirming fake news, an average man can be easily convinced that such is true. This century we live in has been termed a "post-truth" era which entails that it is characterized by "digital disinformation and information warfare led by malevolent actors running false information campaigns to manipulate public opinion.[31] Another issue is that many people are open to anything that confirms their existing views even if they suspect it may be fake. Initially, there were cheap fakes, which entails the use of "low-priced" hardware and they could be easily identified. However, with the availability of deep fake application softwares, high-quality deepfakes can now be made and is accessible with people of little technical skills.

Mike identifies four major possible threats of deepfakes namely; (i)it will put pressure on journalist struggling to filter real from fake news. (ii) it may threaten national security by disseminating propaganda and interfering in elections (iii) it may hamper citizen trust toward information by authorities and (iv) raise cybersecurity issues for people and organizations.[32] It cannot be overemphasized that deepfake will be a threat to national security.[33] Fake videos could cause unrest, riots, protests and violence and conspiracy theories. In respect to deepfake putting pressure on journalists, if nothing is done to regulate deepfakes, at a certain time, even real news will be deemed fake, therefore creating distrust for the media and internet. Extra efforts shall be needed to prove real news, and most times not all efforts may be fruitful. Deepfakes are usually focused on politicians, celebrities, corporate leaders and persons of high repute who can "shake" the internet. Several deepfake videos of political personalities have surfaced; some are for educational purposes while some are blackmail videos. In 2018, a deepfake video of Barack Obama, former US President created by Jordan Peele, a Hollywood filmmaker, mocking President Trump, and discussing the dangers of fake news surfaced. In 2019, an altered video of American politician, Nancy Pelosi which was slowed down to make her sound intoxicated, went viral and had massive outreach.[34] In 2019, the US Democratic Party deepfaked its own Chairman, Tom Perez to highlight

[30] Dave Johnson and Alexander Johnson. (2023, April 5). *What are Deepfakes? How Fake Ai-powered Media can Warp our Perception of Reality.*Business Insider. Retrieved May 17, 2023, from https://www.businessinsider.com/guides/tech/what-is-deepfake?amp

[31] K. E. Anderson. (2018). Getting Acquainted with Social Networks and Apps Combating Fake News on Social Media.*Library Hi-Tech News, 35(3),* 1-6.

[32] Mike Westerland, (supra).

[33] D. Harwell. (2019, June 12).*Top AI Researchers Race to Detect 'Deepfakes' Videos: We are Outgunned.* Washington Post. Retrieved May 7, 2023, from https://www.washingtononpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/.

[34] D. Van Boom.(2019, August 12). *These Deepfakes of Bill Hader are Absolutely Terrifying*.CNET.Retrieved May 3, 2023, from https://www.cnet.com/science/these-deepfakes-of-bill-hader-are-absolutely-terrifying/; C. Towers-

the potential threat of deepfake to the 2020 election.[35] In Central Africa in 2018, an unsuccessful coup by the Gaborone Military was deemed to have been incited by a deepfake of Gabon's long unseen President Ali Bongo, who was believed to be in poor health or dead. In Malaysia, a deep fake clip of a man confessing to having sex with a local cabinet Minister went viral and caused political controversy.[36]

Hany Farid is of the view that deep fakes "have the potential to disrupt societies, economies, and individual lives across the board."[37] He also highlights that through phishing scams powered by deepfakes and targeted to individuals, economies would be disrupted.[38]

The sophistication of this AI technology calls for new laws to curb its use. Some countries and states are taking steps to criminalize the negative use of deep fakes. In the State of Virginia, deep fakes porn or revenge porn is a misdemeanor. The issue with making international regulations or legislations is that they have been known throughout the years to have little effect on malevolent actors, especially foreign states and terrorists that may run massive disinformation campaigns against their State victim on social media platforms.[39] It is noteworthy that development of deepfake regulations and legislations is inconsequential if it is not adopted by the government, media platforms and companies.

Ironically, AI can also be used to detect deep fakes. For instance, AI algorithms can analyze Photo Response Non-Uniformity (PRNU) patterns in footage, that is, imperfection unique to the light sensor of specific camera models or biometric data such as blood flow indicated by subtle changes that occur on a person's face in a video.[40] AI can look at videos on a frame-by-frame basis to track signs of forgery, or renew the entire video at once to examine soft biometric signatures, including inconsistencies in the authenticated relationships between head movements, speech patterns and facial expressions such as smiling to determine if the video has been manipulated.[41]

Some tech experts are of the view that many writers view deepfake from a pessimistic approach, and cannot prove that deepfakes are different from other forms of spreading false information. However, the fact is deep fakes are stronger than all prior means of disseminating false news. Deep fakes are more convincing that mere fake news primarily because of its visual backup. Unlike mere fake news, videos depicting the fake news portrayed are more believable and can be easily recalled. In an experiment, it was ascertained that television viewers were more likely to accurately recall

Clark. (2019, May 31). *Mona Lisa and Nancy Pelosi: The Implications of Deepfakes*.Forbes.Retrieved May 3, 2023, from https://www.forbes.com/sites/charlestowersclark/2019/05/31/mona-lisa-and-nancy-pelosi-the-implications-of-deepfakes/amp/.

[35] D. Van Boom, (supra).

[36] D. Harwell, (supra).

[37]B. Britton. (2023, February 14). *Hany Farid on the Rise of Deepfake Pornography as Twitch Streamers Speak out.* Berkeley School of Information. Retrieved June 30, 2023, from https://www.ischool.berkeley.edu/news/2023/hany-farid-rise-deepfake-pornography-twitch-streamers-speak-out

[38] Ibid.

[39] Mike Westerland, (supra)

[40] J. Andrews, (supra).

[41]C. Carbone. (2019, February 18). *Creepy AI Generates Endless Fake Faces*.Fox News.Retrieved May 9, 2023, from<https://www.foxnews.com/tech/creepy-ai-generates-endless-fake-faces.amp; R. Metz, (supra).

visual messages than verbal messages.[42] Another survey proves that respondents, when recalling events of both visual and verbal information demonstrate higher levels of knowledge.[43] Another study shows that image clips are more powerful in shaping voters' opinion than sound clips.[44] It has also been found that visual information are more convincing and integrated than other types of sensory data. It is easier to process visual information than verbal information. As a matter of fact, based on the "realism heuristic", misleading visuals are more likely to generate false perceptions than verbal content.[45]

Furthermore, individuals treat audio and images as more likely than text to resemble "the real world" of everyday experience. Furthermore, people are more likely to accept messages as true if they perceive them as familiar.[46] Familiarity in this context entails a sense of fluency that makes materials easier to assimilate and therefore more credible.[47] It can be proved that pictures on social media attract more likes and shares and can be spread faster than texts.[48] For instance, images and videos accompanied with tweets from Donald Trump and Hillary Clinton during the 2016 U.S. Presidential campaign received more likes and retweets.[49]The fact is that hyper-realistic deep fakes in its negative form, can either deceive people or make them uncertain about the truthfulness of the content. Where an individual already has a different opinion and sees adeepfake in relation to his opinion, it increases his possibility of believing such a deep fake. Another point is that where a deep fake asserts a thing and there is no immediate contradiction or information available to contradict it, a person is vulnerable to believe such information to be true.[50] Many people are not proficient at detecting deep fakes. Ina study conducted, it was found that:

Individuals who watch a deep fake political video that contains a false statement that is not revealed as false are more likely to be deceived and more likely to experience uncertainty about its content, when compared to users who watch a deep fake political video where the false statement is revealed as true.

---

[42] D.A. Graber. (1990). Seeing is Remembering: How Visually Contribute to Learning from Television News.*Journal of Communication, 40(3),* 134-156.

[43] M. Prior. (2013). Visual Political Knowledge: A Different Road to Competence? *Journal of Politics, 765(1),*41-57.

[44] M.E. Grabe & E.P. Brucy. (2009).*Image Bite Politics: News and the Visual Framing of Election*. Oxford University Press.

[45] I. B. Witten & E.I. Knudseen. (2005).Why Seeing is Believing: Merging Auditory and Visual Worlds.Neuron 48*(3),* 489-496; S.J. Frenda, E.D. Knowles, W. Saletan& E.F. Loftus. (2013). False Memories of Fabricated Political Events.*Journal of Experimental Social Psychology 49(2),* 280-286; S. Sunder. (2008). 'The MAIN Mode: A Heuristic Approach to Understanding Technology Effects on Credibility' in M. Metzger & A. Flanagin (eds.) *Digital Media, Youth and Credibility.* MIT Press.

[46] A.J. Berinsky. (2004).*Silent Voices: Public Opinion and Political Participation in America*. Princeton University Press.

[47] N. Newman, R. Fletcher, A. Kalogeropoulos, D. Levy & R.K. Nielson. (2018). Reuters Institute Digital News Report 2018. *Reuters Institute for the Study of Journalism*.

[48] A. Anderson, J. Hoffman & D.J. Watts. (2015). The Structural Virality Of Online Diffusion. *Management Science 62(1),* 180-196.

[49] E. Pancer & M. Poole. (2016). The Popularity and Virality of Political Social Media: Hashtags, mentions, and Link Predict Likes and Retweets of 2016 US Presidential Nominees' Tweets. *Social Influence 11(4),* 259-270.

[50] Ibid.

In a study conducted on the popular deep fake Obama video,[51] out of 2,005 participants, 50.8% of subjects were not deceived, 16% were deceived, while 33.2% were uncertain.[52] Another issue that affects the growth of deepfakes is whether people go on the internet to check the authenticity of any sensitive video they watch. In the same deep fake Obama experiment, out of 83 persons affirming to have seen the Obama deepfake video, only 35 respondents went on Google to find out more information about the video.[53] The result of this study depicts that political deepfakesmay not necessarily deceive individuals, but may sow uncertainty which may, in turn reduce trust in news on social media.[54]It can be deduced from the result, that if deep fakes remain unchecked the rise of political deepfakes will likely damage online and culture by contributing to a climate of indeterminacy about truth and falsity that, in turn, diminishes trust in online news.[55]

Researchers like Vaccari and Chadwick quantitatively proved deepfakes sow uncertainty and in turn, reduce trust in news seen online.[56] It can lead to serious issues like death. An example is the beating to death of two Indian men, following a video that spread on WhatsApp of two men abducting a child. The mob in North-Eastern Assam State beat the men to death upon belief that the men were the kidnappers. Ironically, the video is not even from India, and it is not even red. It was a child safety awareness clip from Pakistan but where it was made known in the video as an awareness clip was edited out.[57] Hannah Arendt, speaking on the effect of deepfake on trust in social media states: "A people that no longer believes anything cannot make up its own mind. It is deprived of not only its capacity to think and to judge. And with people you can do what you please."[58] John Donegan opines further that "if we cannot trust the content we come across on the internet, there's no limit to the level of disruption we'll encounter."[59]

4.0 An Assessment of Legal Issues and Deep Fake Legislations across Continents

Deep fake is a serious legal issue as it poses a threat not only to journalism and human rights, but also admissibility of evidence, which is the central point of justice. Deep fake leads to several legal issues like cyber harassment, cyber extortion and fraud, online identity theft and intellectual property theft, non-consensual dissemination of pornography, online child sexual exploitation, falsification or manipulation of e-evidence, and distributing disinformation and manipulating public opinion, social unrest and political polarization.[60] In Dubai, a video of a dad threatening his

[51] A deep fake video that shows President Obama calling President Trump a "complete dipshit".

[52] Cristian Vaccari& Andrew Chadwick.(2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty and Trust in News.*Loughborough University*.https://doi.org/10.1177/2056305120903408

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Cristian Vaccari & Andrew Chadwick, (supra).

[57] BBC News. (2018, June 11). *India WhatsApp 'child kidnap' rumours claim two more victims.* Retrieved May 15, 2023, from https://www.bbc.co.uk/news/world-asia-india-44435127.

[58] H. Arendt. (1978, October 26). *Hannah Arendt: From an Interview.*The New York Review of Books. Retrieved May 15, 2023, from https://www.nybooks.com/articles/1978/10/26/hannah-arendt-from-an-interview/

[59] John Donegan. (2022, February 17). *Content Prevanance is our best Chance in the Fight against Deepfakes.* Manage Engine. Retrieved May 16, 2023, from https://www.insights.manageengine.com/artificial-intelligence/content-provenance-is-our-best-chance-in-the-fight-against-deepfakes/

[60] C. Riehle. (2022, May 9). *EuroPol Report Criminal Use of Deepfake Technology.* Eucrim. Retrieved June 27, 2023, from https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/

wife was brought to be tendered as evidence, however, it was discovered to be a deep fake.[61] Deep fake will create a lacuna in the law that makes it easy for anyone to escape liability for videos by raising the issue of authenticity of such video, therefore, giving the prosecution the hard task of proving the authenticity of the video. For instance, in a case between Tesla and Walter Huang which is yet to be decided upon, the basic issue for determination is whether a video of Elon Musk, believed to be acted upon by the deceased Walter Huang was a deepfake or not.[62] Huang's family claimed that the Tesla's driver-assist software failed and was at fault in Huang's death, contrary to a YouTube video made by Musk in 2016 endorsing the driver-assist software, and stating that he would consider "autonomous driving to be basically a solved problem" and "a Model X and Model S, at this point, can drive autonomously with greater safety than a person right now."[63] Currently, Musk's lawyers have raised the issue of deepfake, stating that Musk was a public figure and therefore prone to deepfake videos.

In assessing legislations on deepfake across the globe, it is important to note that there is currently no specific international law on deepfake, therefore, deep fake laws shall be assessed continentally.

United States of America

There is currently no federal United States Deepfake law, but state deep fake legislations exist. In the State of Virginia, deep fake laws focus particularly on deep fake revenge porn and makes it illegal. The Virginia Code Annotated S.182-386.2, specifically outlaws the dissemination of pornographic deep fakes, and also protects against deep fake porn created with the intent to depict an actual person's face or likeness.[64]

The State of Texas has made an explicit law on deepfake called "TXSB751" which illegalizes deep fakes in Texas. This law provides that it is an offense to use deep fake videos, published or distributed within thirty days of an election to injure a candidate or influence the result of an election.[65] It is evident that Texas is more interested in the negative implications of deep lakes in the political aspect. As a matter of fact, the Texas law does not recognize revenge porn as a deep fake. Furthermore, this offense shall be sentenced to up to one year imprisonment and fines up to $4,000.[66]

California's deefake law focuses primarily on eradicating political and pornographic deep fakes. California's deepfake law are contained in Assembly Bill 602 and Assembly Bill 730. Assembly Bill 602 focuses on deepfakes and sexually explicit material. It creates a private cause of action against a person who either intentionally creates or discloses sexually explicit materials, being

[61] P. Ryan. (2020, February 8). *Deepfake Audio Evidence used in U.K. Court to Discredit Dubai Dad.* The National UAE. Retrieved June 27, 2023, from https://www.thenationalnews.com/uae/courts/deepfake-audio-evidence-used-in-uk-court-to-discredit-dubai-dad-1.975764

[62] P. Bandara. (2023, May 8). *Tesla claim Seven Year Old Video of Elon Musk may be a Deepfake.* Petal Pixel. Retrieved June 30, from https://petalpixel.com/2023/05/08/tesla-claim-seven-year-old-video-of-elon-musk-may-be-a-deepfake/

[63] Ibid.

[64] A. Loomis. (2022, April 20). *Deepfakes and American Law*. Davis Political Review. Retrieved June 28, 2023, from https://www.davispoliticalreview.com/article/deepfakes-and-american-law?format=amp

[65] KRW Lawyers. (2019, November 13). *'Deep Fake' Videos under Spotlight of New Texas Law.* Retrieved June 30,2023, from https://www.krwlawyers.com/2019/11/13/deepfake-videos-under-spotlight-of-new-texas-law/

[66] Varghese Summersett. (2021, April 7). *Deep Fakes in Texas: What are they and are they Illegal?* Retrieved June 30, 2023, from https://versustexas.com/deepfakes/

aware that the individual in the material did not give consent, or intentionally discloses sexually explicit materials not created by him, but being aware that the individual in the material did not consent to it. Assembly Bill 730 focuses on deep fakes used to influence political campaigns. This Bill amends the California Election Code to prohibit a person, committee, or other entity from intentionally distributing "materially deceptive audio or visual media " within 60 days of an election, and such material being such that a reasonable man would believe it to be authentic.[67]

Currently, New York has joined the list of US states that have legislations on deep fakes. In the State of New York, there is a recent amendment which now includes deep fake images into its definition of "unlawful dissemination of publication of an intimate image.'[68] The Preventing Deep fakes of Intimate Images Act is aimed at criminalizing digitally altered "intimate" images and provides means of anonymity in institutions of actions for victims.[69] This new Act, just like that of Virginia, focuses primarily on deepfake pornographies.

The problem with curbing deep fake in the United State is its unlimited freedom of speech. Section 230 of the US Communication Decency Act provides that; "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[70] This section generally grants freedom of speech in cyberspace, and it entails that deepfake can be shared and circulated by anyone without accountability and liability. This also entails that the government cannot regulate websites and applications, rather the host or creators will create guidelines for use. This is the major difference between China's deepfake laws and that of the US. The Chinese government has total control over its citizens; access to internet which leads to the effectiveness and smooth running of deep fake laws, unlike in the US where regulation is left to the host and creators of websites and apps, and all these creators usually make different community guidelines, therefore leading to non-uniformity of regulations.[71]

Deep Fake Legislations in Africa

Nigeria

In Nigeria, there is yet to be a specific law recognizing, defining and outlining the implications of deepfake. However, it is noteworthy that the concept of deepfake is a medium through which several cybercrimes which have been provided for in the Cybercrime (Prohibition and protection)

[67] Lexology. (2020, January 20). *California Deepfake Law First in Country to Take Effect.* Retrieved June 30, 2023, from https://lexology.com/library/detail.aspx?g=4700f977-4845-417b-834d-b3c06390ee27

[68] C.A Goldberg. (2023, June 14). *AI Update: FBI Deepfake Warning and New Law*. Retrieved June 27, 2023, from https://www.cagoldberglaw.com/ai-update-fbi-deepfake-warning-and-new-ny-law

[69] J. Gans. (2023, May 5). *NY Democrat Unveils Bill to Criminalize Sharing Deepfake Porn.* The Hill. Retrieved June 29, 2023, from https://thehill.com/homenews/house/3990659-ny-democrat-unveils-bill-to-criminalize-sharing-deepfake-porn/amp/

[70] Section 230, Communication Decency Act.

[71] F. Dauer. (2022, June 29). *Law Enforcement in the Era of Deepfakes*. Police Chief Magazine. Retrieved June 30, 2023, from https://www.policechiefmagazine.org/law-enforcement-era-deepfakes/#google_vignette

Act 2015 are committed.[72] For example, deepfakes can be used to commit cyber defamation,[73] computer related fraud,[74] and identity theft and impersonation.[75]

The Nigerian Cybercrimes Act, 2015, covers certain areas of deep fake malicious usage. Section 12 (2) of the Cybercrime Act criminalizes any act by a person with the intent to defraud via electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss.[76] Section 15 (2) (c) provides that it is an offense for a person via public electronic communications network to transmit any communication "containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person".[77] Section 13 (b)(iii)provides that it is an offense for a person, via a computer system or network to "fraudulently impersonates another entity or person, living or dead, with intent to cause disadvantage to the entity or person being impersonated or another person.[78]

Egypt

Egypt's Dat Al-Ifta, a governmental and non-profit organization that offers Islamic guidance and advice, prohibits the use of Artificial Intelligence to create deep fake video and audios and images. According to it, "it is a lie and deceit contrary to reality and Prophet Mohamed." It further explains that the use of deepfake technology with the intention to deceive or harm another person is contrary to Islam.[79]

Egypt does not have any specific deep fake legislation, however, deepfake actions can be brought under some sections of its Anti-Cyber and Information Technology Crimes Law.[80] This Act, unlike most acts, primarily provides for cybersecurity and data privacy. In Section 26, it criminalizes deliberate acts aimed at processing personal data of a third party to connect such data with an abusive content or to display the same in a way detrimental to the reputation of such third party.[81] It provides in section 25:[82]

Anyone who infringes a family principle or value of the Egyptian society, encroaches on privacy, sends many emails to a certain person without obtaining his/her consent, provides personal data to an e-system or website for promoting commodities or services without getting the approval thereof, or publishes, via the information network or by any means of information technology,

[72] Josephine Uba. (2021, September 23). *Deepfakes in Nigeria: Protection and Legal Framework against Deepfake Attacks in Nigeria*. OlisaAgbakoba Legal. Retrieved June26, 2023, from https://www.mondaq.com/nigeria/security/1114750/deepfakes-in-nigeria-protection-and-legal-framework-against-deepfake-attacks-in-nigeria

[73] Section 15 (2)(c), Cybercrime (Prohibition and Prevention) Act, 2015.

[74] Section 12 (2), Cybercrime (Prohibition and Prevention) Act, 2015.

[75] Section 13, Cybercrime (Prohibition and Prevention) Act, 2015.

[76]Section 12 (2), Cybercrime (Prohibition and Prevention) Act, 2015.

[77] Section 15 (2)(c), Cybercrime (Prohibition and Prevention) Act, 2015

[78]Section 13, Cybercrime (Prohibition and Prevention) Act, 2015.

[79]Ahram Online. (2022, January 7). *Egypt's Dar Al-Ifta Prohibits Deepfake Video and Audio Clips.* Retrieved June 29, 2023, from https://english.ahram.org.eg/NewsContent/1/64/454765/Egypt%E2%80%99s-Dar-AlIfta-prohibts-deepfake-video-and-au.aspx

[80] No. 175 of 2018.

[81] Section 26, Anti-Cyber and Information Technology Crimes LawNo. 175 of 2018.

[82]Section 25, Anti-Cyber and Information Technology Crimes Law No. 175 of 2018.

information, news, images or the like, which infringes the privacy of any person involuntarily, whether the published information is true or false, shall be punishable by imprisonment for no less than six months and a fine of no less than fifty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties.[83]

South Africa

Just like the case of Nigeria, South Africa does not have a specific law regulating the creation and publication of deep fakes, however, liability for deepfake creation and publication may be established using principles in different fields of law.[84] It is noteworthy that the risk of deepfake increases with ignorance. In a survey of 800 respondents between the ages of 18 to 54 from Botswana, Egypt, Kenya, Mauritius and South Africa, conducted by KnowB4, a security software company to determine their awareness of deepfakes, 51% of respondents said they were aware of deepfakes, 28% said they were not aware of deep fakes, 21% were unsure or had a little understanding of what they are.[85]

The Cybercrimes Act of 2020 of South Africa contains sections under which deepfake actions can be brought. Section 5 (3) provides that anyone who interferes with data or a computer program by altering the data or computer program is guilty of an offense.[86] Section 8 criminalizes unlawful acts with the intention to defraud, make a misrepresentation by means of data or a computer program or interference therein, which causes actual or potential prejudice to another person.[87] Section 9 criminalizes the making of false data with the intent to defraud and cause actual or potential prejudice to another person. [88] Finally, Sections 14 and 15 of the Act criminalizes the act of disclosing a data message via electronic communication services, with the intent to incite or threaten a person's or group of persons' property or cause violence against such person or group of persons.[89]

Deep Fake Legislations in Asia

China

China has taken a commendable step in the Asian continent to set up a comprehensive and well-defined legislation of deepfake. China's step is not far-fetched as it is a country with very strict rules on the use of the internet.[90]The Cyberspace Administration of China (CAC) is the regulator behind these rules.[91] China's Regulation on "deepfake synthesis technology" took effect on

[83] Ibid.

[84] N. Mashinini. (2020). The Impact of Deepfakes on the Right to Identity: A South African Perspective. *South African Mercantile Law Journal 32(3)*, 407-436. https//doi.org/10.47348/SAMLJ/v32/i3a5

[85] ADF Magazine. (2023, April 11). *Concerns Grows as 'Deepfakes Spread Misinformation'*. Retrieved June 29, 2023, from https://adf-magazine.com/2023/04/concern-grows-as-deepfakes-spread-misinformation

[86]Section 5 (3), Cybercrimes Act, Act No. 19 of 2020.

[87] Section 8, Cybercrimes Act, Act No. 19 of 2020.

[88] Section 9, Cybercrimes Act, Act No. 19 of 2020.

[89] Sections 14 and 15, Cybercrimes Act, Act No. 19 of 2020.

[90] Asha Hemrajani. (2023, March 8). *China's New Legislation on Deep Fakes: Should the Rest of Asia Follow Suit?* The Diplomat. Retrieved June 30, 2023, from https://thediplomat.com/2023/03/chinas-new-legislation-on-deepfakes-should-the-rest-of-asia-follow-suit/

[91] Arjun Kharpal. (2022, December 22). *China is about to get Tougher on Deep Fakes in an Unprecedented Way. Here's what the Rules Mean.* CNBC. Retrieved June 30, 2023, from https://www.cnbc.com/amp/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes-html.

January 10, 2023. This new regulation is deemed to have two major goals namely; to tighten online censorship and meet up with the rapid advancement of new technologies.[92]

It is noteworthy that mere regulations or legislations on deepfake are not sufficient to control its use. The internet is ubiquitous and for any regulation on it to stand, there must be a solid framework on cyberspace. Trivium explains that China's already existing regulatory system will aid the effectiveness of the deep fake regulation.[93] It explains that China's ability to institute its novel deepfake regulation is hinged on its existing systems that control the transmission of content in online space and regulatory bodies that enforce these rules.[94]

The CAC describes the regulations as necessary because deep synthesis technology "has been used by some unscrupulous people to produce, copy, publish, and disseminate illegal and harmful information, to slander and belittle others' reputation and honor, and to counterfeit others' identities."[95] The regulation contains five chapters with 25 articles that define deep synthesis data and outlines rules managing its use. According to the CAC, deep synthesis technology is one which "employs deep learning, virtual reality, and other synthetic algorithms to produce text, images, audio, video, virtual scenes and other network information."[96] The Deep Synthesis Technology Regulation (DSTR) primarily regulates two entities namely; Deep Synthesis Service Providers, which are companies that offer deep fake services or moreso, provide users with technical support; and the Deep Synthesis Service users, which encompasses both organizations and people who utilize deep synthesis service to create, duplicate, publish or transfer information.[97]

Prior to the DSTR, China had several laws that related to deepfake, for example, the Data Security Law, Personal Information Protection Law, and the 2019 Regulation on the Administration of Online Audio and Video Information Services. China recognises the impact of deepfake on national security and citizens' dignity. Xi Jinping, the President of China in a speech to the Politburo in October 2021, recognized the importance of digital economy and need for technological advancement, but also identifies "unhealthy and uncontrolled symptoms" in the country's digital economy as a serious threat.[98]

It is noteworthy that China's 2019 Regulation on the Administration of Online Audio and Video Information Services had already laid the foundation for deep fake regulation as it forbade the use of computer-generated pictures, audio and video to produce or disseminate rumors.[99] It is also

[92] Ibid.

[93]Trivium China. (2023, May 28). *Deep Dive| China's New Regulations on AI-Generated Content*. Retrieved June 30, 2023, from https://www.triviumchina.com/2023/05/28/deep-dive-chinas-new-regulations-on-ai-generated-content

[94]Trivium China. (2022, February 17). *Deep Dive|Deep(fake) Dive*. Retrieved June 30, 2023, from https://www.triviumchina.com/2022/02/17/deepfakedive

[95] Asha Hemrajani, (supra).

[96] Giulia Interesee. (2022, December 20). *China to Regulate Deep Synthesis (Deepfake) Technology Starting 2023.* China Briefing. Retrieved June 30, 2023, from https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/

[97]Arjun Kharpal, (supra).

[98] R. Creemers, J. Costigan& G. Webster. (2022, January 28). *Xi Jinping's Speech to the Politburo Study Session on the Digital Economy – October 2021*. Digichina. Retrieved June 30, 2023, from https://www.digichina.stanford.edu/work/translation-xi-jinpings-speech-to-the-politburo-study-session-on-the-digital-economy-oct-2021/

[99]Giulia Interesee, (supra).

important to note the provisions of China's deepfake regulation sets out strict rules for Deep Synthesis Service Providers (DSSP) more than deep fake users, and this is so because the DSSP create the medium or platform for deepfake creation and can control the use of its services through its templates and features.

The DSTR comprises four chapters. Chapter I, gives a background to deep fakes and states that the state internet information department is responsible for the overall planning and coordination of the nation's governance of deep synthesis services and related oversight and management efforts.[100] Chapter II outlines regulations for deep synthesis service providers and provides in paragraph 2 of Article 6 that deep synthesis service providers and users must not use deep synthesis services to produce, publish, or transmit fake news information.[101] Chapter III outlines the responsibilities of DSSP, and obliges DSSP that provide services which might cause confusion or mislead the public to make a conspicuous label on information content they generate or edit.[102] Chapter IV outlines the legal responsibility of DSSP[103] and obliges them to undergo a filing process and indicate their filing number on public displayed information on the website or application that they produce.[104]

United Arab Emirates (UAE)

The United Arab Emirates in the Middle East, is still at the stage of creating awareness about the harmful use of deepfake technology. Omar bin Sultan Al Olama, the Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications, explains that it is vital to expose the people to the importance and implications of emerging technologies to build a better future for the next generations. [105]Malicious use of deep fakes in the UAE is on the rise. In 2020, Byron James, a Dubai-based family lawyer revealed that a video presented in court, depicting his client violently threatening his (client) wife was doctored, and upon expert examination, the video was found to be a deepfake.[106] Another example is the use of deep fake voice technology to steal $35million from a bank in UAE in January 2020.[107]

The UAE has launched a deepfake technology guide, via its National Programme for Artificial Intelligence.[108] It is noteworthy that the UAE is fond of utilizing Artificial Intelligence. This guide presents ways to detect fake content using systematic deepfake detection powered by AI-based

[100]Article 2, Provisions on the Administration of Deep Synthesis Internet Information Services, 2022.
[101] Article 6, Provisions on the Administration of Deep Synthesis Internet Information Services, 2022.
[102]Article 17, Provisions on the Administration of Deep Synthesis Internet Information Services, 2022.
[103]Article 19, Provisions on the Administration of Deep Synthesis Internet Information Services, 2022.
[104] China Law Translate. (2022, December 11). *Provisions on the Administration of Deep Synthesis Internet Information Services.* Retrieved June 30, 2023, from https://www.chinalawtranslate.com/deep-synthesis/
[105]
[106] P. Ryan. (2020, February 8). *Deepfake Audio Evidence used in U.K. Court to Discredit Dubai Dad.* The National UAE. Retrieved June 27, 2023, from https://www.thenationalnews.com/uae/courts/deepfake-audio-evidence-used-in-uk-court-to-discredit-dubai-dad-1.975764
[107]Wam, (supra).
[108]Wam. (2021, July 7). *UAE Launches 'Deepfake Guide'*. Khaleej Times. Retrieved June 30, 2023, from https://www.khaleejtimes.com/tech/uae-launches-deepfake-guide?amp=1

tools. The guide classifies fake content into shallow fakes and deep fakes, and offers methods to detect deepfake detection by AI-based tools that are regularly updated.[109]

The deep fake guide outlines the problem with deep fakes, its types, types of forged contents, detection of deepfake, protection from deepfake and the UAE's Digital Wellbeing Council. It identifies deep fake problems to include damage to individual and individual reputation, manipulation of public opinion of the intention of causing disruptions, rise in lack of trust, and creation of fabricated evidence to influence legal judgment. It identifies restriction of personal data as data released in the internet is accessible to everyone, both persons of good faith and malicious persons, and warns that the more data obtained by a malicious actor about a person, the more realistic and believable the deep fake content becomes.

Australia

Australia does not have any specific legislation on deepfake, and no case of deepfake has been brought before any of the Australian courts.[110]The reluctance to establish deepfake laws could be hinged on the fact that there has been no extreme deep fake scandal, and the major malicious actors are based outside Australia.[111] There are several laws in Australia that apply to deep fake.

The Australian Defamation Act[112] covers digitally altered images which creates a solution for deepfaked images.[113] In *Gilbert v. Nationwide News Pty Ltd*,[114] a digitally altered photo of the plaintiff in a newspaper article was held to be a defamation. The Australian Copyright Act of 1968 is among the laws related to deepfake. In copyright law, the creator of a footage is deemed to be the owner of the footage, therefore, reproduction of such footage without prior consent is copyright infringement. However, the complexity of deepfake could frustrate the use of this Act. This is so because through deep fake, the objects, background and even features of the persons in the video or image can be altered, thus creating little or no semblance to the original footage, which now raises the question of whether the deepfake is an original creation. Furthermore, section 29 (1)(a) of the Australian Consumer Law prohibits a person in trade or commerce from making a false or misleading representation that goods or services have sponsorship, approval of a person.[115] However, this only applies to trade or commerce, therefore, deep fakes like revenge porn which is a misrepresentation are not covered.[116]

---

[109]Zawya. (2021, July 7). *The UAE National Programme for Artificial Intelligence Launches a Guide to illustrate Uses of Deepfake Technology.* Retrieved June 27, 2023, from https://www.zawya.com/en/press-release/the-uae-national-program-for-artificial-intelligence-launches-a-guide-to-illustrate-uses-of-deepfake-jb67ph5i

[110] D. Gerakiteys, L. Burke & N. Coulton. (2023, March 24). *Is that you? Deep Dive into Deepfakes Part 2. Legal Issues and Regulatory Landscape.* Clayton UTZ. Retrieved June 30, 2023, from https://www.claytonutz.com/knowledge/2023/march/is-that-you-deep-dive-into-deepfakes-part-2-legal-issues-and-regulatory-landscape

[111] Ibid.

[112] N0. 77, 2005.

[113] White Knight Lawyers. (2022, 1 May). *Deepfake Technology: Current Remedies and Possible Legal Consequences.* Retrieved June 30, 2023 from https://wkls.com.au/deepfake-technology-current-remedies-and-possible-legal-consequences

[114] (2016) NSWSC 845

[115] White Knight Lawyers, (supra).

[116] White Knight Lawyers, (supra).

The United Kingdom (U.K.)

The United Kingdom has established deep fake legislations, although the legislation primarily focuses on revenge porn. The Online Safety Bill is the primary deep fake legislation in the United Kingdom. Prior to this legislation, lawyers prosecuting deep fake cases had to prove that the malicious actor had the intent to cause distress to malicious actors which is exceedingly hard, and failure to do so, the malicious actor would go free, even though it was proven that he made a misleading deep fake video. With this legislation, whether intent to cause distress is proved or not, there is a punishment for making a misleading deep fake video. Successful proof of intent will lead to two years imprisonment of the actor, but failure to prove intent with proof of creation of misleading deepfake will lead to six months imprisonment of the malicious actor.

The Lord Chancellor, Alex Chalk, KC is in full support of the legislation as he believes that it will put an end to humiliation of women via manipulated intimate pictures and videos.[117]Paul Scully, the U.K. The Minister of Technology and Digital Economy, states that deep fake porn and intimate photos have a devastating impact on the lives of women and girls across the U.K.[118]

The U.K.'s Online Safety Bill outlines responsibilities of deep fake service providers. It charges them with the responsibility of user-identification verification to ensure that malicious deep fakes are traced to their creators. It also charges the deep fake service providers with children's risk assessment and adult risk assessment to ensure that contents on their website or software applications do not facilitate child sexual exploitation and abuse and are not detrimental to adults' dignity (by sharing revenge porn). Particularly in Section 13 (4), it requires that contents harmful to adults be: (i) taken down; (ii) users' access to such content be restricted; (iii) there should be limited recommendation and promotion of such content.[119]

International Convention on Deep Fakes

At the moment, there is no international convention against deep fakes. The United Nations Institute for Disarmament Research (UNIDIR) 2021 Innovations Dialogue on Deepfakes, Trust and International Security was held in Geneva on 25th August 2021. The event explored the importance of trust for international security and stability and shed light on how the growing deep fakes phenomenon could undermine this trust. As a result, the U.S. and its democratic allies should consider developing a code of conduct for deepfake use by governments, drawing on existing international norms and precedents.

5.0 CONCLUSION AND RECOMMENDATIONS

Conclusion

The problem with the detection of deepfakes is that any weakness identified by researchers in deepfake is immediately improved, and also, people and resources invested in developing deepfake

[117] Rachel Thompson. (2023, June 27). *Sharing Deepfake Porn Criminalised in England and Wales*. Mashable. Retrieved June 28, 2023, from https://mashable.com/article/deepfake-porn-criminalised
[118] H. Saddique. (2023, June 27). *Sharing Deepfake Intimate Images to be Criminalized in England and Wales.* The Guardian. Retrieved June 28, 2023, from https://amp.theguardian.com/society/2023/jun/27/sharing-deepfake-intimate-images-to-be-criminalised-in-england-and-wales
[119] Section 13 (4), Online Safety Bill.

technologies supersede those working to overpower it.[120] Deepfake malicious actors consistently improve their techniques, and making laws to keep up with them is difficult. Nevertheless, big tech companies are spending resources to detect deep fakes. Facebook is doing so through its Deep Fake Detection Challenge and Google though its Deep Fake ban.[121]Identifying deepfakes is not an easy task. According to Nina Schick, who wrote the book "Deep Fakes" in 2020, we will never be able to detect all manipulated content."[122]Hao Li concurs with Schick and states that it will soon be absolutely impossible to detect deep fake, and this is as a result of the upgrades made by deep fake makers and researchers. There is still uncertainty of whether deepfakes should be totally eradicated or ignored. However, if deepfakes are left unchallenged, it could have profound implications for journalism, citizen competence, and the quality of democracy.[123]

Although deep fakes are events that never occurred, but they have real consequences. They can inflict psychological harm on the victim, reduce employability and affect relationships. This is also a medium for cybercriminals to conduct fraud stress-free. However, deep fake threat to national security is less frequent, however theoretical, it is possible. For instance, supposed Russian actors disseminated a deep fake videos that showed Ukrainian President, Volodymr Zelensky telling his military to stand down it was however quickly removed by social media companies.

Furthermore, deepfakes can be used to assert or consolidate dangerous thinking. The problem is even if a person debunks a deep fake, it is unlikely that it will reach out to the many that have seen or believed this.[124] The need to establish both national and international legislations to regulate and supervise the use of deepfakes cannot be overemphasized. Putting an end to deep fake absolutely will be unethical because of its positive impact, especially in the film industry and putting motion on dead people to soothe their loved ones, however, leaving it unchallenged entails a world of uncertainties and distrust. The onus is on both International organizations and national institutions to set up specific legislations to ensure that before deep fakes become ubiquitous, they are controlled.

Recommendations

Educating people on deep fake is crucial. Many people are unaware of deep fakes, and public awareness should be raised urgently. Digital literacy of the community should be facilitated to help people detect fake videos, images and footages at least, in the least technical way possible. This is necessary because even if experts are able to detect deep fakes, and the people are not, such

[120] Tonya Riley.(2019, June 13). *The Technology 202: Its Time for Congress to Address Deepfakes, Experts say.*Washington Post.Retrieved May 17, 2023, from https://www.washingtonpost.com/news/powerp ost/paloma/the-technology-202/2019/06/13/the-technology-202-it-s-time-for-congress-to-address-deepfakes-experts-say/5d01687aa7a0a4586bb2da85/

[121] Jack Cook. (2022, July 27). *Deepfake Technology: Assessing Security Risk.* American University.Retrieved May 15, 2023, fromhttps://www.american.edu/sis/centers/security-technology/deepfake-technology-assessing-security-risk.cfm

[122] Nina Schick. (2020).*Deepfakes: The Coming Infocalypse.* Hachette Book Group.

[123] W.L. Bennett & S. Livingstone. (2018). The Disinformation Era: Disruptive Communication and the Decline of Democratic Institution. *European Journal of Communication 33(2),* 122-139.

[124] Debra Bruce. (2021, September 15). *Applications of Deepfake Technology: Positives and Dangers.* Knowledge Nile. Retrieved May 15, 2023, from https://www.knowledgenile.com/blogs/applications-of-deepfake-technology-positives-and-dangers/; MehhmaMagh. (2022, February 18). *To see no Longer Means to Believe: The Harms and Benefits of Deepfake.* Retrieved May 15, 2023, from https://www.ethics.org.au/to-see-no-longer-means-to-believe-the-harms-and-benefits-of-deepfake/.

detection is of no positive value because the videos are to be watched by the people. It should be noted that anyone can be deepfaked, and there are also simple picture and video taking techniques that one could employ to avoid being easily deepfaked, or even deepfaked at all. For instance, having obstruction, such as waving hands in front of a face in a photo or video can provide some protection.[125]

Cybersecurity: With deep fake, cybersecurity strategies need an immediate upgrade. Social engineering, that is the use of spam emails or calls, pretending to be a relative of a person or someone close to the person to extort money from such a person, will become upgraded to an almost undetectable mode. With deep fakes, a cybercriminal can perfectly mimic the voices of a potential victim's relative or boss to extort money. Furthermore, companies, governments, and authorities using facial recognition technology and storing vast amounts of facial data for security and verification purposes, need to address the threat of identity theft of such data, were it to be leaked.[126] This implies that stronger cybersecurity measures need to be adopted to ensure that such sensitive data is not leaked.

Adopting a video authentication process prior to posting it on the internet is necessary. A video authentication process can be programmed to ensure that everyone uses it prior to posting, hence non-users' videos or images will be flagged down as non-authentic and the identity of deep fake persons can be revealed. Messages from verified pages on social media can be believed since the poster can be held responsible for the news. However, with Elon Musk's new move of selling verification tags (blue ticks) on Twitter, this can grow the deep fake community, since they can just buy the tick and make their videos even more convincing, as people would deem it authentic since it is shared by a verified page. Fact-checking by social media companies also aids in the control of deep fakes. Fact-checking is very hard as the number of videos and images being uploaded exceed the software and human resources used to verify them. For instance, users upload 500 hours of content per minute on YouTube, and Twitter struggles with 8 million accounts that attempt to spread content through manipulative techniques.

Lastly, but most importantly, specific legislation must be put in place to control deep fake. These legislations must be all encompassing, that is, they must cover all aspect sf deepfakes. For example, it is evident that Virginia's deepfake laws mainly concentrate on deep fake pornography or revenge porn. A comprehensive deep fake legislation, pointing out the several deep fake malicious acts and consequences, like China's Deep Synthesis Technology Regulation is advised. Furthermore, in this context, the law is no longer regarded as solely the last hope of the ordinary man, but the last hope of preserving trust in media, sustaining global and national security, maintaining security on the internet and safeguarding human dignity. Firstly, deep fake application softwares can be banned, since they are what makes deep fake accessible to numerous bad actors. Laws can be put in place to criminalize fake videos of events or persons that never happened. It should also be an offense for someone to share a video without fact-checking. If people can be held responsible for videos they share, deep fake makers, although they enjoy anonymity on the internet, will become frustrated. When one person is punished for sharing a fake video, then another would exercise

[125] J.E. Solsman (2019, April 4). *Deepfakes may Ruin the World. And they can come for you, too.*CNET.Retrieved May 15, 2023, from https://www.cnet.com/google-amp/news/deepfakes-may-try-to-ruin-the-world-but-they-can-come-for-you-too/
[126] Towers-Clark, (supra),

caution before sharing a video. Every social media user should be held responsible for whatever information they share on their accounts. This might be deemed restrictive, but it is better than lawlessness on the internet.

REFERENCES

[1] ADF Magazine. (2023, April 11). *Concerns Grows as 'Deep Fakes Spread Misinformation'*. Retrieved June 29, 2023, from https://adf-magazine.com/2023/04/concern-grows-as-deepfakes-spread-misinformation

[2] Ahram Online. (2022, January 7). *Egypt's Dar Al-Ifta Prohibits Deepfake Video and Audio Clips.* Retrieved June 29, 2023, from https://english.ahram.org.eg/NewsContent/1/64/454765/Egypt%E2%80%99s-Dar-AlIfta-prohibts-deepfake-video-and-au.aspx

[3] Anderson, A. and Hoffman, J. and Watts, D.J.(2015). The Structural Virality Of Online Diffusion. *Management Science 62(1),* 180-196.

[4] Anderson, K.E.(2018). Getting Acquainted with Social Networks and Apps Combating Fake News on Social Media.*Library Hi-Tech News, 35(3),* 1-6.

[5] Andrews, J. (2019, July 12). *Fake News is Reality – A.I. is going to make it much Worse?* USA Today. Retrieved May 6, 2023, from https://www.cnbc.com/amp/2019/07/12/fake-news-is-real-ai-is-going-to-make-it-much-worse.html.

[6] Arendt, H.(1978, October 26). *Hannah Arendt: From an Interview.*The New York Review of Books. Retrieved May 15, 2023, from https://www.nybooks.com/articles/1978/10/26/hannah-arendt-from-an-interview/

[7] Bandara, P. (2023, May 8). *Tesla claims Seven Year Old Video of Elon Musk may be a Deepfake.* Petal Pixel. Retrieved June 30, from https://petalpixel.com/2023/05/08/tesla-claim-seven-year-old-video-of-elon-musk-may-be-a-deepfake/

[8] Barney, N. '(n.d.). *Deep Fake AI (deepfake)*. Techtarget. Retrieved May 8, 2023, fromhttps://www.techtarget.com/whatis/definition/deepfake

[9] BBC News, (2018, June 11). *India WhatsApp 'child kidnap' Rumors claim two more Victims.* Retrieved May 15, 2023, from https://www.bbc.co.uk/news/world-asia-india-44435127.

[10] Bennett, W.L. & Livingstone, S. (2018). The Disinformation Era: Disruptive Communication and the Decline of Democratic Institution. *European Journal of Communication 33(2),* 122-139.

[11] Berinsky, A.J.(2004).*Silent Voices: Public Opinion and Political Participation in America*. Princeton University Press.

[12] Berkowitz, J. (2019, October 7).*There are almost 15k Deepfake Videos out there- and 96% of them are porn.* Facts Company. Retrieved May 14, 2023, from https://www.fastcompany.com/90414116/there-are-almost-15k-deepfake-videos-out-there-and-96-of-them-are-porn

[13] Boom D. V.(2019, August 12). *These Deepfakes of Bill Hader are Absolutely Terrifying.*CNET.Retrieved May 3, 2023, from https://www.cnet.com/science/these-deepfakes-of-bill-hader-are-absolutely-terrifying/

[14] Brandon, J. (2018, February 16).*Terrifying High-Tech Porn Creepy "Deep Fake" Videos are on the Rise.*Fox News. Retrieved May 8, 2023, fromhttps://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise

[15] Britton, B. (2021, March 5). *Deep Fake Videos of Tom Cruise went Viral. Their Creator Hopes they Boost Awareness.*NBC News.Retrieved May 17, 2023, from https://www.nbcnews.com/tech/tech-news/creator-viral-tom-cruise-deepfakes-speaks-rcna356

[16] Britton, B. (2023, February 14). *Hany Farid on the Rise of Deepfake Pornography as Twitch Streamers Speak out.* Berkeley School of Information. Retrieved June 30, 2023, from https://www.ischool.berkeley.edu/news/2023/hany-farid-rise-deepfake-pornography-twitch-streamers-speak-out

[17] Bruce, D. (2021, September 15). *Applications of Deepfake Technology: Positives and Dangers.* Knowledge Nile. Retrieved May 15, 2023, from https://www.knowledgenile.com/blogs/applications-of-deepfake-technology-positives-and-dangers/

[18] Cambridge Dictionary. (n.d.). *Deepfake*. Retrieved May 8, 2023, from https://dictionary.cambridge.org/dictionary/english/deepfake

[19] Carbone, C. (2019, February 18). *Creepy AI Generates Endless Fake Faces*.Fox News.Retrieved May 9, 2023, from https://www.foxnews.com/tech/creepy-ai-generates-endless-fake-faces.amp

[20] China Law Translate. (2022, December 11). *Provisions on the Administration of Deep Synthesis Internet Information Services.* Retrieved June 30, 2023, from https://www.chinalawtranslate.com/deep-synthesis/

[21] Chivers, T. (2019, June 23).*What do we do about Deep Fake Video?*The Guardian. Retrieved May 6, 2023, from https://amp.guardian.com/technology/2019/jun/23/what-do-we-do-about-deepfake-video-ai-facebook

[22] Chow, M. (2022, June 9). *What are the Positive Applications of Deep Fake?* Jumpstart Magazine. Retrieved May 14, 2023, from https://www.jumpstartmag.com/what-are-the-positive-applications-of-deepfakes/

[23] Cook, J.(2022, July 27). *Deepfake Technology: Assessing Security Risk.* American University.Retrieved May 15, 2023, from https://www.american.edu/sis/centers/security-technology/deepfake-technology-assessing-security-risk.cfm

[24] Creemers , R., Costigan, J. & Webster, G. (2022, January 28). *Xi Jinping's Speech to the Politburo Study Session on the Digital Economy – October 2021*. Digichina. Retrieved June 30, 2023, from https://www.digichina.stanford.edu/work/translation-xi-jinpings-speech-to-the-politburo-study-session-on-the-digital-economy-oct-2021/

[25] Dauer, F. (2022, June 29). *Law Enforcement in the Era of Deepfakes*. Police Chief Magazine. Retrieved June 30, 2023, from https://www.policechiefmagazine.org/law-enforcement-era-deepfakes/#google_vignette

[26] Dickson, B.(2018, June 7). *When AI Blurs the Line between Reality and Fiction.*PC Magazine.Retrieved May 8, 2023, from https://www.pcmag.com/news/when-ai-blurs-the-line-between-reality-and-fiction

[27] Donegan, J. (2022, February 17). *Content Prevanance is our best Chance in the Fight against Deepfakes.* Manage Engine. Retrieved May 16, 2023, from

https://www.insights.manageengine.com/artificial-intelligence/content-provenance-is-our-best-chance-in-the-fight-against-deepfakes/

[28] Eddy, M. and Rubenking, N.(2019, August 9). *Detecting Deep Fakes may Mean Reading Lips*. PCM Magazine.Retrieved May 6, 2023, from https://www.pcmag.com/news/detecting-deep fakes-may-mean-reading-lips

[29] Evans, C. (2018, April 17). *Spotting Fake News in a World with Manipulated Videos.*CBS News. Retrieved May 6, 2023, from https://www.cbsnews.com/amp/news/spotting-fake-news-in-a-world-with-manipulated-video/.

[30] Ferrier, E.(2022, 24 June). *The Pros and Cons of Deep Fake Technology Google News gets a redesign Tiktok's Platform Strategy Revealed, and Instagram's Main Feed to be revamped.* Intelligence.Retrieved May 14, 2023, from https://www.intelligencygroup.com/blog/digital-roundup-24-6-22

[31] Fletcher, J. (2018). Deep Fakes Artificial Intelligence and some kind of Dystopia: The New Faces of Online Post-Fact Performance.*Theatre Journal 70 (4)*, 455-471. DOI: 10.1353/tj.2018.0097.

[32] Frenda, S.J., Knowles, E.D., Saletan, W. & Loftus, E.F. (2013). False Memories of Fabricated Political Events.*Journal of Experimental Social Psychology 49(2)*, 280-286.

[33] Gans, J. (2023, May 5). *NY Democrat Unveils Bill to Criminalize Sharing Deepfake Porn.* The Hill. Retrieved June 29, 2023, from https://thehill.com/homenews/house/3990659-ny-democrat-unveils-bill-to-criminalize-sharing-deepfake-porn/amp/

[34] Gerakiteys, D., Burke, L. & Coulton, N. (2023, March 24). *Is that you? Deep Dive into Deepfakes Part 2. Legal Issues and Regulatory Landscape.* Clayton UTZ. Retrieved June 30, 2023, from https://www.claytonutz.com/knowledge/2023/march/is-that-you-deep-dive-into-deepfakes-part-2-legal-issues-and-regulatory-landscape

[35] Gilbert, D. (2023, March 8). *High Schoolers made a Racist Deep Fake of a Principal Threatening Black Students.*Vice.Retrieved May 2, 2023, fromhttps://www.vice.com/enarticle/7kX2R9/school-principal-deepfake-racist-video

[36] Goldberg , C.A. (2023, June 14). *AI Update: FBI Deepfake Warning and New Law*. Retrieved June 27, 2023, from https://www.cagoldberglaw.com/ai-update-fbi-deepfake-warning-and-new-ny-law

[37] Gonzalez, O. (2019, June 25).*Instagram Chief Adam Mosseri: We don't have a Policy against Deepfakes*.*CNET*.Retrieved May 5, 2023, from https://www.cnet.com/google-amp/news/instagram-chief-adam-mosseri-we-dont-have-a-policy-against-deepfakes/

[38] Grabe, M.E. & Brucy, E.P.(2009).*Image Bite Politics: News and the Visual Framing of Election*. Oxford University Press.

[39] Graber, D.E. (1990). Seeing is Remembering: How Visually Contribute to Learning from Television News.*Journal of Communication, 40(3)*, 134-156.

[40] Harwell, D. (2019, June 12).*Top AI Researchers Race to Detect 'Deepfakes' Videos: We are Outgunned.* Washington Post. Retrieved May 7, 2023, from

https://www.washingtononpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/

[41] Hern, A. (2018, March 12). *My May-Thatcher Deepfake won't Fool you but its Tech may change the World.*The GuardianRetrieved May 6, 2023, from https://amp.theguardina.com/technology/2018/mar/12/may-thatcher-deepfake-face-swap-tech-change-world

[42] Hemrajani, A. (2023, March 8). *China's New Legislation on Deep Fakes: Should the Rest of Asia Follow Suit?* The Diplomat. Retrieved June 30, 2023, from https://thediplomat.com/2023/03/chinas-new-legislation-on-deepfakes-should-the-rest-of-asia-follow-suit/

[43] Interesse, G. (2022, December 20). *China to Regulate Deep Synthesis (Deepfake) Technology Starting 2023.* China Briefing. Retrieved June 30, 2023, from https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/

[44] Johnson, D. and Johnson, A. (2023, April 5). *What are Deep Fakes? How Fake Ai-powered Media can Warp our Perception of Reality.* Business Insider. Retrieved May 17, 2023, from https://www.businessinsider.com/guides/tech/what-is-deepfake?amp

[45] Kan, M. (2018, September 17). *U.S. Lawmakers: AI Generated Fake Videos may be a Security Threat*. PC Magazine. Retrieved May 6, 2023, from https://ww.pcmag.com/news/us-lawmakers-ai-generated-fake-videos-may-be-a-security-threat

[46] Kharpal, A. (2022, December 22). *China is about to get Tougher on Deep Fakes in an Unprecedented Way. Here's what the Rules Mean.* CNBC. Retrieved June 30, 2023, from https://www.cnbc.com/amp/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes-html.

[47] KRW Lawyers. (2019, November 13). *'Deep Fake' Videos under Spotlight of New Texas Law*. Retrieved June 30, 2023, from https://www.krwlawyers.com/2019/11/13/deepfake-videos-under-spotlight-of-new-texas-law/

[48] Lexology. (2020, January 20). *California Deepfake Law First in Country to Take Effect.* Retrieved June 30, 2023, from https://lexology.com/library/detail.aspx?g=4700f977-4845-417b-834d-b3c06390ee27

[49] Loomis, A. (2022, April 20). *Deepfakes and American Law*. Davis Political Review. Retrieved June 28, 2023, from https://www.davispoliticalreview.com/article/deepfakes-and-american-law?format=amp

[50] Magh, M. (2022, February 18). *To see no Longer Means to Believe: The Harms and Benefits of Deepfake.* Retrieved May 15, 2023, from https://www.ethics.org.au/to-see-no-longer-means-to-believe-the-harms-and-benefits-of-deepfake/

[51] Maras, M. and Alexandrou, A. (2019). Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deep Fake Videos. *International Journal of Evidence and Proof (23)(3)*. 255-262. DOI: 10.1177/1365712718807226

[52] Mashinini, N. (2020). The Impact of Deep Fakes on the Right to Identity: A South African Perspective. *South African Mercantile Law Journal 32(3),* 407-436. https//doi.org/10.47348/SAMLJ/v32/i3a5

[53] Metz, R. (2019, June 12).*The Fight to Stay ahead of Deepfake before the 2020 US Election.CBN.*Retrieved May 6, 2023, fromhttps://www.amp.cnn.com/cnn/2019/06/12/tech/deepfake-2020-detection/index.html

[54] Newcastle University.(2019, 14 June). *Newcastle Expert to Explore the Rise of Deepfakes*. Retrieved May 17, 2023, fromhttps://www.ncl.ac.uk/press/articles/archive/2019/06/deepfakrsbarbicantalk/

[55] Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D. & Nielson, R.K. (2018). Reuters Institute Digital News Report 2018. *Reuters Institute for the Study of Journalism*.

[56] Noone, G. (2021, July 12). *How to Win the War on Deep Fakes*. Retrieved May 17, 2023, from https://techmonitor.ai/technology/ai-and-automation/how-to-win-the-war-on-deepfakes-detecting

[57] O'Sullivan, D. '(2019, August 10). *The Democratic Party Deepfaked its own Chairman to Highlight 2020 Concerns.*CNN. Retrieved May 17, 2023, from https://amp.cnn.com/cnn/2019/08/09/tech/deefake-tom-perez-dnc-defcon/index.html

[58] Pancer, E. and Poole, M. (2016). The Popularity and Virality of Political Social Media: Hashtags, mentions, and Link Predict Likes and Retweets of 2016 US Presidential Nominees' Tweets. *Social Influence 11(4)*, 259-270.

[59] Patterson, D. (2019, June 13). *From Deepfake to "Cheap Fake," it's Getting Harder to tell what's true on your Favorite Apps and Websites.*CBN News.Retrieved May 17, 2023, from https://www.cbsnews.com/amp/news/what-are-deepfakes-how-to-tell-if-video-is-fake/

[60] Prior, M. (2013). Visual Political Knowledge: A Different Road to Competence? *Journal of Politics, 765(1),*41-57.

[61] Riehle, C. (2022, May 9). *EuroPol Report Criminal Use of Deepfake Technology.* Eucrim. Retrieved June 27, 2023, from https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/

[62] Riley, T. (2019, June 13). *The Technology 202: Its Time for Congress to Address Deepfakes, Experts say.*Washington Post.Retrieved May 17, 2023, from https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/06/13/the-technology-202-it-s-time-for-congress-to-address-deepfakes-experts-say/5d01687aa7a0a4586bb2da85/

[63] Ryan, P. (2020, February 8). *Deepfake Audio Evidence used in U.K. Court to Discredit Dubai Dad.*The National UAE. Retrieved June 27, 2023, from https://www.thenationalnews.com/uae/courts/deepfake-audio-evidence-used-in-uk-court-to-discredit-dubai-dad-1.975764

[64] Saddique, H. (2023, June 27). *Sharing Deep Fake Intimate Images to be Criminalized in England and Wales.* The Guardian. Retrieved June 28, 2023, from https://amp.theguardian.com/society/2023/jun/27/sharing-deepfake-intimate-images-to-be-criminalised-in-england-and-wales

[65] Sample, I. (2020, January 13). *What are Deepfakes and how can you Spot them?*The Guardian.Retrieved May 8, 2023 from https://amp.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

[66] Schick, N. (2020). *Deepfakes: The Coming Infocalypse.* Hachette Book Group.

[67] Solsman, J.E. (2019, April 4). *Deepfakes may Ruin the World. And they can come for you, too.*CNET.Retrieved May 15, 2023, from https://www.cnet.com/google-amp/news/deepfakes-may-try-to-ruin-the-world-but-they-can-come-for-you-too/

[68] Solsman, J.E. (2019, May 24). *Samsung Deepfake AI could Fabricate a Video of you from a Single Profile Picture.* CNET. Retrieved May 6, 2023, fromhttps://www.cnet.com.com/google-amp/news/samsung-ai-deepfake-can-fabricate-a-video-of-you-from-a-single-photo-mona-lisa-cheapfake-dumbfake/

[69] Summersett, V. (2021, April 7). *Deepfakes in Texas: What are they and are they Illegal?* Retrieved June 30, 2023, from https://versustexas.com/deepfakes/

[70] Sunder, S. (2008). 'The MAIN Mode: A Heuristic Approach to Understanding Technology Effects on Credibility' in M. Metzger & A. Flanagin (eds.) *Digital Media, Youth and Credibility.* MIT Press.

[71] Thompson, R. (2023, June 27). *Sharing Deepfake Porn Criminalised in England and Wales*. Mashable. Retrieved June 28, 2023, from https://mashable.com/article/deepfake-porn-criminalised

[72] Towers-Clark, C. (2019, May 31). *Mona Lisa and Nancy Pelosi: The Implications of Deepfakes*.Forbes.Retrieved May 3, 2023, from https://www.forbes.com/sites/charlestowersclark/2019/05/31/mona-lisa-and-nancy-pelosi-the-implications-of-deepfakes/amp/

[73] Trivium China. (2022, February 17). *Deep Dive|Deep(fake) Dive*. Retrieved June 30, 2023, from https://www.triviumchina.com/2022/02/17/deepfakedive

[74] Trivium China. (2023, May 28). *Deep Dive| China's New Regulations on AI-Generated Content*. Retrieved June 30, 2023, from https://www.triviumchina.com/2023/05/28/deep-dive-chinas-new-regulations-on-ai-generated-content

[75] Uba, J. (2021, September 23). *Deepfakes in Nigeria: Protection and Legal Framework against Deepfake Attacks in Nigeria*. Olisa Agbakoba Legal. Retrieved June 26, 2023, from https://www.mondaq.com/nigeria/security/1114750/deepfakes-in-nigeria-protection-and-legal-framework-against-deepfake-attacks-in-nigeria

[76] Vaccari, C. & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty and Trust in News. *Loughborough University.* https://doi.org/10.1177/2056305120903408

[77] Wam. (2021, July 7). *UAE Launches 'Deepfake Guide'*. Khaleej Times. Retrieved June 30, 2023, from https://www.khaleejtimes.com/tech/uae-launches-deepfake-guide?amp=1

[78] Westerland, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Information Management Review(9)(11),* 39-52.

[79] White Knight Lawyers. (2022, 1 May). *Deepfake Technology: Current Remedies and Possible Legal Consequences.* Retrieved June 30, 2023 from https://wkls.com.au/deepfake-technology-current-remedies-and-possible-legal-consequences

[80] Witten, I.B. & Knudsen, E.I. (2005). Why Seeing is Believing: Merging Auditory and Visual Worlds. *Neuron 48(3),* 489-496.

[81] Zawya. (2021, July 7). *The UAE National Programme for Artificial Intelligence Launches a Guide to illustrate Uses of Deepfake Technology*. Retrieved June 27, 2023, from https://www.zawya.com/en/press-release/the-uae-national-program-for-artificial-intelligence-launches-a-guide-to-illustrate-uses-of-deepfake-jb67ph5i