Module Code: CS3SC16

Assignment report Title: Technical Report

Student number (e.g. 25098635): 29015642

Date (when the work completed): 30/12/22

Actual hrs spent for the assignment: 28 hours

Assignment evaluation (3 key points):

- Required a lot of researching and learning into the area of deepfake
- Took much longer than expected to write up the final part of the report
- Coursework specification was a bit vague.

Contents

1. Abstract

Deepfake technology presents significant social, legal and ethical challenges. Recently, the term "deepfake" has become more prevalent than ever. Deepfakes refer to the face-swapping technology that makes it possible to produce realistic synthetic photos or movies. In the age of video and audio production, the ability to produce realistic-looking and sounding files offers unprecedented opportunities for deception. Studies regarding the ethical ramifications of deepfakes raise concerns about their potential use for blackmail, intimidation, sabotage, ideological influence, and incitement to violence. By looking into the four categories of deepfakes; pornography, political campaigns, commercial uses, and creative use, this report will critically analyse the social, legal and ethical interpretations of the use of deepfake technology. In addition, we will discuss how companies and individuals deal with deepfakes and how this affects them.

2. Introduction

Deep fakes, otherwise known as synthetic media, is a term used to describe hyper realistic media types, such as photos, videos, and audio. Machine learning and artificial intelligence fuel deep fakes by inputting various factual information and producing 'real' media. As soon as rapid interest in the area sparked in the year of 2017, the word 'deepfake' was coined [0]. The revolution of deepfake was established when an anonymous user posted a machine learning algorithm that used previously existing artificial intelligence algorithms to create videos that appeared realistic but were fake [1]. After this algorithm's source code was made publicly available, thousands of people shared it on the Internet. As a result, videos including celebrity faces could be easily transposed into pornographic videos.

Although, the whole idea of deepfakes is not a new discovery. During the 1990s, researchers had already conducted academic research on computer vision and video manipulation [2]. However, they lacked the processing power and resources to compute the models efficiently and successfully. In those days, artificial intelligence and machine learning were just theories that would eventually be implemented.

A generative adversarial network (GAN), which can be split into two machine-learning models, is used to create deepfake videos [3]. The first model includes the creation of the fake video from a vast data set of sample videos, whilst the other detects if the fraudulent video is fake so that the deepfake video can be believable enough that the human cannot tell if it is a deepfake. An algorithm produces a value that, if it exceeds a certain threshold, the media created can be accepted by a human as being realistic. A larger dataset generally results in better performance of GANs. This is why deepfake media of celebrities and politicians appear much more realistic since the GAN can create synthetic media more quickly and accurately.

A critical analysis of the social effects of deepfake media is provided in the report, analysing how deepfake media threatens society's interpersonal relations, attitudes and impacts by analysing the pros and cons associated with deepfake media. Furthermore, this report discusses the legal issues associated with deepfakes, including how companies may exploit copyright infringements to remove deepfake content, defamation, and how current laws cannot provide direct protection against deepfake technology misuse. Lastly, the report examines the ethical aspects of deepfake, critically evaluating the impacts on an individual's life and mental health and discusses media companies' moral responsibilities when removing deepfake content from their platforms. To support the points made, various case studies and examples are provided to provide a much clearer and more in-depth understanding of this new era.

3.1 Social

It is important not to underestimate the potential harm that can be caused by deepfakes. They are used to create fake news, false pornographic videos and malicious hoaxes that usually target celebrities and politicians. As the algorithms for deepfake are considered open source, thousands of spin-off applications now use deepfake technology in unique ways [4]. FaceApp is a free mobile application with over 500 million users worldwide [5]. The app has a toolset of artificial intelligence filters, backgrounds and effects that can transform images/videos into deepfakes. Since these technologies are so publicly available, there is room for manipulation and misuse of deepfake. Although there might be a severe problem with deepfake, upsides to this equipment include creating entertaining and exciting content. As BuzzFeed reviewed FaceApp, they stated: “Honestly, this will probably make your entire day”, suggesting that the impact of using the deep fake capabilities was uplifting and gave a positive externality to society [6]. In addition, Vogue also made a publication stating, “sharing a picture of your future wrinkled self has been one of 2019’s biggest crazes.” [7]. In other words, deepfakes may be used for the good of society and as a means of experimenting with the technology.

However, there always bears a threat where if something is potentially powerful, evil is always lurking around the corner. When looking at some specific downsides of deepfake, because of the versatility of deepfake technology, there may be room for severe damage. Fake pornography videos are being created through the utilisation of deepfake. In this case, the face of the person in the pornographic film is replaced with the face of the person targeted in the pornographic film. In a review of the consequences of deepfake, Noelle Martin explains the realistic effects on someone [8]. He states that the repercussions can stay with a victim for their entire life as images and videos are near impossible to remove from the internet once they are on there. He details how it would affect your interpersonal relations and job interviews. A Revenge Porn Helpline, funded by the UK government, received a case in which a teacher had lost their job after being victimised to deepfake pornographic images of herself that were circulated throughout social media [9]. Her school learned of this, and they were forced to terminate her position as a teacher because this media violated company policy, even though it was a deepfake. This clearly illustrates the social impact of deepfakes and how they can cause significant harm to the lives of people.

Though deepfake has negative externalities, companies can use the technology to increase productivity and reduce costs. JustEat is a company founded in demark, and its duties are to provide food deliveries from restaurants and supermarkets [10]. It is one of the top performers for food deliveries in the UK, standing next to Deliveroo and UberEats. JustEat’s marketing team teamed up with Snoop Dog to create a short music video which includes an advertisement for their services [11]. In Australia, JustEat is called MenuLog, and the marking team only created one video to represent Snoop Dog with their new advertising technique. JustEat had two choices: create a new video of Snoop Dog singing MenuLog instead of JustEat or hire an AI deepfake company to utilise deepfake technology to edit the video so that Snoop Dogg says MenuLog instead. The costs of creating an entirely new music video would be much greater than hiring a company to edit the existing video. In this case, the company Synthesia was responsible for creating it; they did not just swap out logos but also changed Snoop's lip movements and facial expressions [12]. As a result, AI and deepfake software can be utilized to reduce costs and ultimately increase profits in the industrial sector. Deepfake has also been applied to the entertainment industry, whereby actors do not need to be in person; they can use a digital representation of the actor [13]. This can benefit the

production team as they can make the actor do anything they want without the actor making mistakes such as saying the wrong word or doing the incorrect action, resulting in the reduction of reshooting the videos as the team can just edit the deepfakes accordingly.

A significant consequence of deepfake is the ability to demolish people's lives using fake content. Every year, as technology advances in this area, it becomes increasingly difficult to determine what is real and what is fake [14]. The results of experiments reported by Sophie J. Nightingale and Hany Farid in a study published indicate that the average person cannot distinguish between fake and natural imagery and that synthetic media were even rated more realistic than real media in terms of 'realism' [15]. The accuracy rate of 315 participants was just below 48.2% when comparing a deepfake and a natural person [16]. The results are astonishing since this number is nearly 50%, indicating that the participants had difficulty choosing between the images. Companies are developing artificial intelligence that can detect deepfake images to combat the threat of synthetic media rapidly evolving and lurking in the lives of ordinary people. Sentinel is a tech start-up from Estonia whose critical business goal is to assist governments, and media companies defend against fake media [17]. For the detection of deepfake content, the company has developed several algorithms. A primary method of detecting deepfakes is the Defence in Depth approach, which utilizes multiple layers of defence based on a vast database of deepfake content classified using neural network algorithms to detect deepfakes accurately. In light of this, there may be a solution to the problem of fake media. Despite this, most social media sites do not have this type of validation or removal of deepfakes.

3.2 Legal

When considering the legal aspects of deepfakes, there is a problem: deepfakes are a relatively new technology, and laws must be directly enacted to combat them. It should be noted, however, that there are currently no laws that specifically address deepfake. Therefore, existing laws are being used to combat deepfakes at the moment. According to a recent interview from Vouge, deepfake technology was used to portray Kim Kardashian on YouTube [18]. This video was removed by YouTube due to "Copyright Grounds" under the requirements of the Digital Millennium Copyright Act. DMCA is a legal act that amends the original copyright law to address the relationship between copyright and the internet [19]. Section 512 of this act provides that copyright owners may have "infringing online content removed without litigation". Therefore, the owners of Vouge were entitled to act in the manner they did. However, the creators of the deep fakes may argue that their intent was "fair use". The term "fair use" refers to the act of using someone else's artwork or content without their permission to create your own content, make a parody, or mock it [20]. As Winston Cho explains, "fair use" is determined by four factors: the intent and character of the work, its nature and sustainability, and its effects on the potential market [21]. Unfortunately, there is a more significant obstacle here; a copyright claim must exceed the level of fair use to be legally pursued. Despite the difficulty in proving this fact, deep fakes are likely to avoid lawsuits since they can claim "fair use" for the material they have created.

During the 2018 elections, a deep fake video of Pelosi was used to alter how she spoke to make it appear that she was intoxicated [22]. It was achieved by having an algorithm slur her words and make longer pauses between sentences. The origin of the original video was unclear, but it was quickly shared across social media. Social media erupted with this Tweet, racking up 12 million views within a short period of time. Citizens of America thought the video content was accurate because most captions claimed she was drunk. Therefore, the general public lost trust in the candidate and voted for other candidates. She suffered a great deal of damage to her reputation and her potential to run as a candidate in the future. This is a pure example of defamation. Defamation can be defined as a false statement that causes harm to another person or another person's reputation [23]. Pelosi's reputation was ruined; therefore, she could have filed a lawsuit for defamation. However, the person who produced the video was never found; hence she could not file a lawsuit against a particular party. Because deepfake is a new technology and the nature of this case is how it is, it was tough for the culprit to plead guilty. It is important to note that, in defence of

the creators, it is almost impossible for a public figure to win a defamation suit unless they can prove actual malice [24]. If Nancy Pelosi brought a defamation lawsuit against the creators, she would have to prove that they acted with actual malice and that the deepfakers had the actual intent to harm her reputation. In this case, it might be possible, but it requires a substantial burden of proof which is very hard to get.

Deepfakers might use someone's image to attempt to make monetary gains. They could do this by putting the images on t-shirts, tv, and political and internet advertisements, which allows them to capitalise on someone's image without their permission. Rihanna had recently conflicted with top shop as they were using her image on their t shirts as a marketing campaign [25]. Rihanna pressed charged against them and won the case. Resulting in top shop removing her images and having to pay a large sum. Although, in most cases, this would rise to a cause of action, violating the right of publicity. There is, however, a defence to this: the first amendment, which guarantees freedom of speech to human beings [26]. Deepfakers will defend any claim about the right to publicity, saying that they have the right to say what they want unless it is harmful to the public. In this situation, denying them, they have the right to free speech hard. They are sending a message by doing these deepfake videos sending a serious message or a satirical message. They are exercising their 1st amendment, which is freedom of speech, on this deepfake content. However, deepfakers could continue to create explicit or dangerous deep fake media without being concerned about being prosecuted. When extreme measures are taken, such as in cases of terrorism threats, the US government will take legal action as this matter is taken seriously.

3.3 Ethical

It will be claimed that while deepfakes may provide positive benefits to society, they are nevertheless unethical. Whether or not the person(s) being portrayed would disagree with how they are depicted, whether the deepfake misleads viewers, and the intended purpose of the deepfake all play a role in how morally questionable a particular deepfake is. Deepfakes can be morally incorrect because they exploit digital data that represents people's voice and/or picture to represent them in ways they would not want to be represented. Individuals who object to being deepfaked are deprived of their fundamental right to control how their image and voice, which play a vital role in defining their identity, are represented realistically through the digital representation of their images and voices. Deepfakes present hyper-realistic depictions of people over whom they had no control, drastically disrupting the interpersonal processes through which a person's identity is socially constructed. In the age of deepfakes, protection from the manipulation of digital representations of our face and voice should be viewed as a fundamental moral right because they are directly related to our social and personal identities.

One major problem with deepfakes is that they can mimic a person's likeness without consent. Deepfakes are being used to merge photos and videos of a person with pornographic media to create sexual gratification. This is considered wrong as the person targeted is being used as a source of pleasure and entertainment without their consent. In 2019, an app called DeepNude utilised the technology and was able to create this type of media [27]. Not only did the original developer take down the app due to excessive traffic, but they also stated that "the probability that users will misuse it is too high". This indicates that the company was aware of the potential problems and immoral uses of the application. Users were manipulating images purposely to inflict harm, humiliate or damage other people's reputation. Even so to the point of revenge porn whereby potentially broken relationships attempt to humiliate each other by creating deepfake pornography. This issue is much more prevalent than other potential harms of deepfake as it was found that from a study, 96% of existing deepfake content takes the form of pornography [28]. This form of pornography has a low probability of being consensual, which is why it poses a significant problem in today's society. By amending its online safety bill, the United Kingdom Government plan to completely ban non-consensual deepfake pornography [29]. However, the ability to create more photos/videos is getting easier and easier each year as the process of creating deepfakes becomes faster and more efficient due to breakthroughs in new algorithms and computer specifications. The psychological effect on an individual inflicted with deepfake pornography can be life changing. There is

a possibility that deepfakes can cause significant emotional distress and damage to lives. A teacher from a school was victimised by deepfake pornography, crumbling her career and her interpersonal relations [30]. Clearly, this was not a moral thing to do. Perhaps the consequentialism of this was not as intended, as the teacher had to deal with severe consequences for being of the victim of these actions. The example above illustrates how powerful deepfake can be and how it can be used to destroy a person's identity and life.

When creating and distributing deepfake content, the creators must ensure that the synthetic media is ethical. Tech companies such as Google and Microsoft, which have the tools to create deepfake media very fast, have moral obligations [31]. These obligations are aimed at preventing harm. While the people who use the software are responsible for sharing and consuming the content, they still have a primary role in effectively responding to malicious deepfakes by reporting or flagging content. Nevertheless, despite this, the company providing the platform must show ethical and social responsibility towards using deepfakes on their platform. Websites, even today, are struggling to regulate deepfake content due to their ability to stay hidden and blend into what we perceive as natural media. In 2018, Pornhub, a popular pornography streaming website, banned deepfake content on their platform, yet they could not fully regulate deepfakes [32]. In 2019, after the ban on deepfakes, A pornographic deepfake video of Ariana Grande was viewed over 9 million times before it was taken down [33]. One of the main problems with this video is that it did not explicitly state that the video was a deepfake but was still uploaded like any other video. Therefore, the content was hidden away on Pornhub's servers until some users flagged it for deepfake content. This shows that even if a company follows their moral responsibilities, it can still be challenging to regulate its policies. This is because it can almost be impossible to predict human actions before they upload content. In addition, the algorithms used before uploading content are not advanced enough to detect deepfake content. Perhaps in a few more years, as deepfake detection applications are created and distributed, platforms will have algorithms capable of detecting deepfake content to remove or label it.

Based on deontology, deepfake technology appears to be morally problematic as it is intended to deceive. Deception in this context refers to the ability to violate truthfulness and risk the ability for people to pursue actions related to their own will. When looking at the dictionary definition of deception, it states that [34] "the act of causing someone to accept as true or valid what is false or invalid" This implies that for an action to relate to deception, someone must need to accept that the presented material by the deceiver is true/valid and what is false/invalid. When relating this to deepfake technology, for it to be morally problematic, deepfakes need to convince the viewer of the content the content that it is real but, it is fake. An example of this could be uploading a deepfake content and the owner of that content states that the media is real and is not a deepfake, then the viewer of the content believing that it is real. Deepfake has been used to facilitate fraud whereby in 2019 the voice of a CEO was synthetically used to transfer funds [35]. This is a pure example of deception as the bank owners were deceived to the point where they believed that it was actually the CEO talking but in reality, it was a scammer that had used deep fake technology to forge the voice. This goes to show the potential of deepfake and how it could be used for much worse.

4. Conclusion

In conclusion, the crossover between digital media and Artificial Intelligence has dramatically impacted modern society. Deepfakes have become weaponizable to the point that they could have a massive influence on the economic world. Due to the power of deepfake, the public has lost trust in what they perceive as real or fake since deepfake media can stay hidden with a cloak of the appearance of it being a natural media source. The goal for society now is for the people and the authorities to properly understand the power and potential of deepfake by adequately addressing the challenges associated with deepfake and preventing any misuse of its toolset. Within the analysis of this report, evidently, the inclusion of deepfake technology in the digital media era has had several impacts on not only individuals but also big technology firms.

Throughout the social section of this report, we examined the potential benefit or harm of deepfakes to society. One section analysed the monetary gain for businesses. JustEat used deepfake technology to change Snoop Dog's mouth and lyrics without employing Snoop Dog again for an entirely new music video.

This significantly reduced their company costs as the marketing team only had to reach out to a deepfake company that charged a considerably low amount when comparing the cost of creating an entirely new video. There are many more examples that were not mentioned in this report; however, the central ideology of this concept applies to any company with similar issues. Although, there were some negative effects on society, such that a teacher's career and life were crushed due to deepfake pornography. Someone had face-swapped this teacher's face on the face of women on pornographic content, and the results were so realistic that the school she was working at had to terminate her contract. Not only did this have a negative impact on her life, but also on her students that she taught at the time as they had just lost their teacher, which can be a complex problem for some students, especially in terms of their learning and their future. There are, in fact, remedies to deepfake technology; however, the level of deepfake detection is not entirely publicly available. Deepfake is not currently sanctioned by UK or US government (as of now), so cases such as the teacher's incident will not be verified as proving innocent when victimised by deepfakes. These remedies are only being used in the defence sector in other governments around the world, and companies that are researching these remedies, such as Sentinel, are only tech start-ups. Unfortunately, these companies are only working for the governments and not the commercial sector as of now, so the ability to filter social media platforms will continue to be a prevalent issue.

Regarding the legal side of deepfakes, it was found that no natural laws counter deepfake technology; however, existing laws are being utilised to stand against deepfake content. This section detailed how tech companies such as YouTube and Facebook are counteracting deepfake content by using laws such as copyright infringement to take down media that has been deepfaked. The analysis also discussed that the deepfakers can defend themselves from lawsuits and legal action by pleading their human rights and the “fair use” act. It is almost impossible to prove that someone had created content intended to defame or ruin someone’s reputation. This is a severe issue, as deepfakers can continue to create harmful content and not get prosecuted for it. Due to the fact that deepfake technology is so open source and publicly available, it would be almost impossible for governments to sanction deepfake content, especially because it is tough to determine between what is real and fake media. It is necessary to adjust the law behind deepfakes for the sake of society and the lives of the individuals affected.

The ethical section critically analysed consequentialism, virtue ethics and care ethics by relating to moral responsibilities. Big tech companies must have moral obligations to take down content that targets an individual with fake news or uses harassment. However, the responsibility is also to the creator of the deepfake content to label it as a deepfake or even the viewer of the content to report it if the media threatens individuals or provides false information. It was also found that it is important to understand that deepfakes have the power to be used for fraudulent activities, which could be used to destroy someone’s life. There do need to be specific algorithms set in place to prevent situations such as fraud. In addition, the significant impacts of deepfakes are down to how we use them and label the content. Deepfakes are a potent tool that should not be misused or misjudged.

To finalise, deeper analysis is needed when discussing the legal side of deepfakes. This report briefly describes some legalities relating to deepfake technology, but there are many more. The government should consider enacting more laws in the future to combat deepfake so the individuals creating the explicit, illegal content can be prosecuted, which then has the knock-on effect to prevent future instances of deepfake misuse.

5. Reflection on Learning

When starting this assignment, I was scared and unsure of how or where to begin. After reading a few articles and watching some videos related to the list of potential topics we could talk about, I decided to pick deepfake as I had recently heard about it in the news, and I became incredibly interested in the area. I decided to start reading publications directly related to deepfakes and I got a grasp of what deepfake was and how it can be used. What I did find challenging was finding the content that related to social, legal and ethical factors of deepfake. The articles I found online for these were very vague and I felt as though they

were giving me the wrong information. I feel as though I spent the majority of my time researching and trying to find suitable sources for me to analysis and discussion. In terms of the overall report, in computer science, we don't usually write essays, so this was a bit of a challenge for me to get the effort and motivation to start writing. However, I could work swiftly through the assignment when I came into the correct zone. I did really enjoy this assignment as I feel as though I have not only learned a lot about deepfakes, but I have also learned core assignment writing fundamentals. However, I struggled with the vagueness of the report description. I was unclear about what the mark scheme was asking for and was a bit confused about how much to write and what style to write in. Fortunately, the university provides templates and tutorials on how to write an analytical essay. I found this content helpful when structuring and writing my essay. Throughout my assignment, I learned the core base of the understanding of what deepfake is and how it can be used to manipulate people and businesses as well as the media. What I found particularly shocking was that deepfake has been around for many years now, and yet the government has not set laws directly to tackle it. I do expect the government to generate laws that will tackle deepfakes, as the technology is rapidly evolving every year. I believe we will go into an age where deepfakes are so realistic that we will be unable to tell what is real and what is fake online ever again.

In terms of the lectures, I had attended conducted by Pat, I found them incredibly inciteful and interesting. This is because of the open-lecture style of teaching that Pat does. He engages with us a lot, asking us questions and allowing us to discuss specific topics with each other and him. Due to this fact, I have understood a lot more about not only the social, legal and ethical side of computer science but also a lot more when it comes to working in the industry and communicating with my peers and my lecturer. Another thing that was very interesting was the fact that he used real-world case studies as examples to back up his points in the theory. Quite a few lectures were spent reviewing case studies, and I found these lectures most valuable since I could understand how all these SLE conditions affect businesses in the real world. What particularly interested me was when, as a cohort, we reviewed the case study with SAS and WLP about how WLP used some of SAS's code for their almost homogenous product, and SAS tried to pursue legal action. It was fascinating to learn the story behind this and how it confirms that the software's functionality is not protected by copyright. I will be applying the information and skills that I have gained from this module into my future job, career and lifestyle.

6. References

[0] books.google.com. (n.d.). Google Books Ngram Viewer. [online] Available at: https://books.google.com/ngrams/graph?content=deepfake&year_start=1800&year_end=2019&corpus=26&smoothing=3 [Accessed 29 Nov. 2022].

[1] Deepfake Now. (2020). Deepfake History: When Was Deepfake Technology Invented? [online] Available at: https://deepfakenow.com/deepfake-history-when-invented/#:~:text=the%20term%20%E2%80%98deepfake%E2%80%99- [Accessed 1 Dec. 2022].

[2] Wikipedia. (2022). Deepfake. [online] Available at: https://en.wikipedia.org/wiki/Deepfake#:~:text=beginning%20in%20the- [Accessed 1 Dec. 2022].

[3] Techslang — Tech Explained in Simple Terms. (2019). Deepfake Technology: What is It and How does It Work? — Techslang. [online] Available at: https://www.techslang.com/what-is-deepfake-technology/.

[4] eSafety Commissioner. (2021). Deepfake trends and challenges — position statement | eSafety Commissioner. [online] Available at: https://www.esafety.gov.au/industry/tech-trends-and-challenges/deepfakes.

[5] faceapp.com. (n.d.). FaceApp - AI Face Editor. [online] Available at: https://www.faceapp.com/.

[6] Garafano, L. (n.d.). Here's What 33 Celebrities Look Like With FaceApp's 'Old' Filter. [online] BuzzFeed. Available at: https://www.buzzfeed.com/laurengarafano/celebs-with-faceapp-old-age-filter [Accessed 30 Nov. 2022].

[7] Nast, C. (2019). This is how Instagram and Snapchat filters are changing the future of makeup. [online] Vogue India. Available at: https://www.vogue.in/beauty/content/makeup-trends-instagram-snapchat-filters-changing-the-future-of-makeup#:~:text=sharing%20a%20picture%20of%20your%20future%20wrinkled%20self%20has%20been%20one%20of%202019%E2%80%99s%20biggest%20crazes [Accessed 30 Nov. 2022].

[8] MIT Technology Review. (n.d.). A horrifying new AI app swaps women into porn videos with a click. [online] Available at: https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/#:~:text=what%20I%20do.-.

[9] MIT Technology Review. (n.d.). A horrifying new AI app swaps women into porn videos with a click. [online] Available at: https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/#:~:text=UK%20government%20recently%20received%20a%20case%20from%20a%20teacher [Accessed 1 Dec. 2022].

[10] Takeaway. (n.d.). Just Eat Takeaway.com | Leading online food delivery marketplace. [online] Available at: https://www.justeattakeaway.com/

[11] flare (2020). 3 New Ways Artificial Intelligence Is Powering The Future Of Marketing - Nitrobots. [online] Nitrobots. Available at: https://nitrobots.ai/3-new-ways-artificial-intelligence-is-powering-the-future-of-marketing/ [Accessed 1 Dec. 2022].

[12] flare (2020). 3 New Ways Artificial Intelligence Is Powering The Future Of Marketing - Nitrobots. [online] Nitrobots. Available at: https://nitrobots.ai/3-new-ways-artificial-intelligence-is-powering-the-future-of-marketing/#:~:text=With- [Accessed 1 Dec. 2022].

[13] Intelligency Group | Digital Intelligence & Marketing. (2022). 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. [online] Available at: https://www.intelligencygroup.com/blog/digital-roundup-24-6-22/#:~:text=in%2Dperson%20actor.- [Accessed 1 Dec. 2022].

[14] Salpekar, O. (n.d.). DeepFake Image Detection. [online] Available at: http://cs230.stanford.edu/projects_spring_2020/reports/38857501.pdf [Accessed 1 Dec. 2022].

[15] Nightingale, S.J. and Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. Proceedings of the National Academy of Sciences, 119(8), p.e2120481119. doi:10.1073/pnas.2120481119.

[16] We can't tell apart deepfakes from real people but we 'trust' them more. (n.d.). We can't tell apart deepfakes from real people but we 'trust' them more. [online] Available at: https://www.trtworld.com/magazine/we-can-t-tell-apart-deepfakes-from-real-people-but-we-trust-them-more-55037#:~:text=accuracy%20rate%20of- [Accessed 1 Dec. 2022].

[17] Insights, S. (2020). 5 Top Startups Tackling Deepfakes | StartUs Insights Research. [online] StartUs Insights. Available at: https://www.startus-insights.com/innovators-guide/5-top-startups-tackling-deepfakes/#:~:text=using%20AI%20techniques.- [Accessed 1 Dec. 2022].

[18] Li, T.C. (2019). This Backdoor Approach to Combating Deepfakes Won't Work. [online] Slate Magazine. Available at: https://slate.com/technology/2019/06/deepfake-kim-kardashian-copyright-law-fair-use.html#:~:text=Recently%2C%20there%20have [Accessed 1 Dec. 2022].

[19] U.S. Copyright Office (n.d.). The Digital Millennium Copyright Act | U.S. Copyright Office. [online] www.copyright.gov. Available at: https://www.copyright.gov/dmca/.

[20] www.youtube.com. (n.d.). DEEPFAKE Videos - The Emerging Legal NIGHTMARE!!! [online] Available at: https://www.youtube.com/watch?v=pr7_KySn-Bs [Accessed 19 Jun. 2021].

[21] Cho, W. and Cho, W. (2022). Does Kendrick Lamar Run Afoul of Copyright Law by Using Deepfakes in 'The Heart Part 5'? [online] The Hollywood Reporter. Available at: https://www.hollywoodreporter.com/business/digital/does-kendrick-lamar-run-afoul-of-copyright-law-by-using-deepfakes-in-the-heart-part-5-1235145596/.

[22] www.youtube.com. (n.d.). DEEPFAKE Videos - The Emerging Legal NIGHTMARE!!! [online] Available at: https://youtu.be/pr7_KySn-Bs?t=187 [Accessed 1 Dec. 2022].

[23] McMillan LLP. (2018). What Can The Law Do About 'Deepfake'? [online] Available at: https://mcmillan.ca/insights/what-can-the-law-do-about-deepfake/#:~:text=Intellectual%20Property%20Rights.- [Accessed 1 Dec. 2022].

[24] www.youtube.com. (n.d.). DEEPFAKE Videos - The Emerging Legal NIGHTMARE!!! [online] Available at: https://youtu.be/pr7_KySn-Bs?t=231 [Accessed 1 Dec. 2022].

[25] Rihanna wins Topshop T-shirt court case. (2013). BBC News. [online] 31 Jul. Available at: https://www.bbc.co.uk/news/entertainment-arts-23514738.

[26] The White House (2021). The Constitution. [online] The White House. Available at: https://www.whitehouse.gov/about-the-white-house/our-government/the-constitution/.

[27] Samuel, S. (2019). AI deepfake app DeepNude transformed photos of women into nudes. [online] Vox. Available at: https://www.vox.com/2019/6/27/18761639/ai-deepfake-deepnude-app-nude-women-porn.

[28] HT Tech. (2019). 96% of deepfake videos online contain porn: Study. [online] Available at: https://tech.hindustantimes.com/tech/news/96-of-deepfake-videos-online-contain-porn-study-story-T2L4b03B1gmxtwhn7cTgKO.html [Accessed 1 Dec. 2022].

[29] Engadget. (n.d.). UK aims to ban non-consensual deepfake porn in Online Safety Bill. [online] Available at: https://www.engadget.com/deepfake-porn-uk-ban-online-safety-bill-171007700.html [Accessed 1 Dec. 2022].

[30] MIT Technology Review. (n.d.). A horrifying new AI app swaps women into porn videos with a click. [online] Available at: https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/#:~:text=case%20from%20a- [Accessed 1 Dec. 2022].

[31] Lane, M. (2020). Responsible Innovation: The Next Wave of Design Thinking. [online] Medium. Available at: https://medium.com/microsoft-design/responsible-innovation-the-next-wave-of-design-thinking-86bc9e9a8ae8.

[32] The Independent. (2018). Pornhub bans AI-generated ‘deepfakes’ videos that put female celebrities into porn films. [online] Available at: https://www.independent.co.uk/tech/pornhub-twitter-deepfakes-ban-ai-celebrity-faces-porn-actress-bodies-emma-watson-jennifer-lawrence-a8199131.html [Accessed 1 Dec. 2022].

[33] Prindle Institute. (n.d.). deepfake Archives. [online] Available at: https://www.prindleinstitute.org/tag/deepfake/#:~:text=Popular%20pornography%20website%2C- [Accessed 1 Dec. 2022].

[34] www.merriam-webster.com. (n.d.). Definition of DECEPTION. [online] Available at: https://www.merriam-webster.com/dictionary/deception#:~:text=the%20act%20of%20causing%20someone%20to%20accept%20as%20true%20or%20valid%20what%20is%20false%20or%20invalid%20%3A%20the%20act%20of%20deceiving [Accessed 1 Dec. 2022].

[35] www.marsh.com. (n.d.). Marsh | Global Leader in Insurance Broking and Risk Management. [online] Available at: https://www.marsh.com. [Accessed 1 Dec. 2022].