Journal of International Women's Studies

Volume 25
Issue 2 *4th Global Conference on Women's Studies Special Issue: Mapping Uncharted Pathways in Contemporary Women's Studies*

Article 11

March 2023

Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns

Chidera Okolie
University of East Anglia, England

Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns

By Chidera Okolie[1]

Abstract

Artificial Intelligence (AI) is a phenomenon that has become embedded in human life, and this symbiotic relationship between technology and humanity is here to stay. One such use of AI is deepfakes. The use of AI for deepfakes is arguably one of the most controversial topics because it raises ethical issues. Deepfakes are images or recordings that have been convincingly altered and manipulated to misrepresent someone as doing or saying something that they did not actually do or say. These manipulations thrive in the political arena and recently in the pornography industry, in which women's faces are masked onto other bodies to create video illusions that cause non-consensual sexual-image abuse and other harms. It is no surprise that the malicious use of deepfake technology has prompted regulatory legislation like the United States National Defense Authorization Act (NDAA), and the recent ratification of amendments to the Digital Services Act (DSA) on criminalizing malicious deepfakes. Scholars, advocates, and victims continue to call for more specific and stricter laws to regulate deepfakes and assign penalties for non-adherence. This paper presents a timely analysis of deepfake pornography as a type of image-based sexual abuse, and of the position of the law on malicious use of deepfake technology. Data protection concerns under the General Data Protection Regulation, and policy recommendations and measures for redress, control, and eradication are also addressed.

Keywords: Artificial Intelligence, Cyberbullying, Deepfakes, Digital Media, Ethics, Law, Image manipulation, Sexual abuse

Introduction

Digital technology, while not an instrument of harm on its own, nevertheless poses the possibility of exploitation and harm. One of these digital technologies is Artificial Intelligence (AI) technology. It is a branch of computer science which involves developing computer programs to complete tasks which would otherwise require human intelligence (Saleh, 2019). AI is a tool for revolutionized inventions in healthcare (Greig, 2021), education, communication, and finance, yet it can also be weaponized for nefarious activities, such as cybercrimes (phishing scams and advance fee frauds), cyberstalking, and bullying (Burrell & Fourcade, 2021). Some of the results of these crimes have been loss of finances, reputation, and in extreme cases, lives. It has become evident that the good versus evil attributes of digital technology are dependent on the individual in whose hands these technologies find expression. After all, in the seeming uncertainty of AI technology, one thing has remained certain to date: until fully autonomous AI technologies are developed, AI is still completely reliant on human manipulation.

AI also finds expression in the media industry, where it is widely used to create video edits through dynamically transposing one image (or a series of similar images) onto a

[1] Chidera Okolie is a Development Professional with six years' experience in Business/Project Management, research, legal compliance, and public speaking. She is currently a Cybersecurity Analyst, and a career enthusiast in Data Protection, Responsible AI, and policy. She is a graduate of law from the University of Nigeria, a Solicitor, and is currently completing her Masters in Information Technology and Intellectual Property Law at the University of East Anglia, England. She considers herself adaptable, resourceful and insightful. She also loves to read, paint, listen to jazz and explore culinary terrains. She is a published fiction author of two books. She can be contact by email at c.okolie@uea.ac.uk

secondary source (e. g., a still or motion picture). This gives the indistinguishable illusion that an individual is engaging in an action that in reality is not the case. These illusions are called deepfakes. Deepfake technology is widely used in the pornography industry, where illusions of sexual acts are created (Fido et al., 2022; Li et al., 2019; Rofer, 2017). To better understand the AI-altered videos called synthetic media and how deepfake technology can be used to perpetrate image-based sexual abuse, we will give some background on image-based sexual abuse as a whole, AI, and how it works to create deepfakes. We will then explore deepfake pornography in-depth.

Image-Based Sexual Abuse

When we think about sexual abuse, we often imagine a scenario where physical force is exerted to elicit sexual satisfaction, usually in the form of molestation or rape. While this is a form of sexual abuse in itself, which we will not review in depth for the purpose of this study, a more menacing approach to sexual abuse has infiltrated the digital space because of its nature for ease of perpetuation and the untold damage caused to its victim. This form of sexual abuse is called image-based sexual abuse, which refers to non-consensual creation, display, and distribution of sexual images (Ringrose et al. 2022).

The law states that the intention behind this dissemination must be to cause harm to the victim. The UK Revenge Pornography Guideline (UKRPG) from January 2017 provides thus:

> A person will only be guilty of the offence if the reason for disclosing the photograph, or one of reasons, is to cause distress to a person depicted in the photograph or film. On the same basis, anyone who re-tweets or forwards without consent, a private sexual photograph or film would only be committing an offence if the purpose, or one of the purposes was to cause distress to the individual depicted in the photograph or film who had not consented to the disclosure. For example, anyone who sends the message only because he or she thought it was funny would not be committing the offence (UKRPG, 2017).

The rationale behind this section may be to exclude the non-prejudicial dissemination of explicit content for other intents like entertainment, which may not in itself absolve the offender of any form of liability. Yet, it can only be pleaded as a defense for mitigation of punishment where no other malicious intent is established or be brought under a different law such as the law of tort.

Image-based sexual abuse is classified under sexual offenses and policies for legislative reform for the purposes of filling in the gaps between this type of abuse and other sexual offenses, of identifying patterns, and of making important connections. Why is there a need to make this connection? The nature of image-based sexual abuse is such that while the mode of abuse might differ in methodologies, what remains similar are the intentions, causes, and impacts on victims such as trauma, societal victim-shaming, and damage to reputation. Clare McGlynn & Erika Rackley (2017) provide a rationale for this synthesis by noting that where there is an understanding of image-based sexual abuse as a part of the wider whole of sexual abuses, the necessary support for victims of any type of sexual violence is spread across all forms, and we can adopt a wider approach in suggesting coherent strategies and policies against all forms of sexual abuse. The purpose of this synthesis-approach could also be understood to eradicate hierarchy in forms of sexual violence and to bring all forms of sexual violence, whether physical or virtual, under one umbrella with each accorded as much priority as the other.

The dissemination of the explicit material that forms content for image-based abuse usually takes two forms: offline, where the material is physically shown to other people through

interactions with a live audience; or online, through various means such as uploads to email, social media, or pornographic sites.

The UKRPG 2017 further ensures this wider approach and scope by extending the offense to apply to any kind of disclosure of private sexual photographs or films (assuming that the other criteria in the offense are satisfied). This could include uploading images on the internet, sharing by text or email, or showing someone a physical image. This means that where there is evidence of malicious intention under the UKRPG 2017, a determination of image-based sexual abuse will be upheld irrespective of the chosen mode or platform for dissemination.

Nicola Henry and Asher Flynn (2019) posited three main categories of activities that account for an image-based sexual abuse: non-consensual recording; taking of nude or sexual images; non-consensual distribution, sharing, posting, or dissemination of nude or sexual images, whether online or offline or both; and sextortion, the making of threats to share nude or sexual images, where threats may be communicated in person or via cell phone, email, apps, or internet sites. Today, we can add the creation and manipulation of data to create digital clones for pornography purposes with the use of deepfake technology.

Motivations of the Perpetrators

While we will not fully exhaust the motivations behind every instance of criminal sexual abuse, there appears to be patterns that have been drawn in the past between criminals and the intentions behind their actions, although the list of patterns is not exhaustive. While the perpetrators of image-based sexual abuse are usually known to have had nefarious motives from the start, there have been cases where the act was perpetrated by family and friends with no known motives. In a study by Vasileia Karasavva & Adelle Forth (2022), 56.9% of those who experienced such abuse and victimization reported that one or more of their perpetrators were their intimate or ex-partners. Another 64.3% of reported one or more of their perpetrators were their friends or family members, and 15.9% reported they did not know who their perpetrators were. This means there are varied motivations behind image-based abuse which could span from revenge by different perpetrators like ex-partners to aggrieved family members to sexual gratification and circumvention of consent by total strangers. Below are common motivations of the perpetrators of image-based sexual violence.

Sexual Pleasure

One of the most reoccurring motives for image-based sexual abuse is to elicit satisfaction through physical and/or psychological stimulation of senses.

Bullying through Power Exertion

This is where the abuser repeatedly causes psychological and emotional harm to the victim of image-based sexual abuse simply because they can (or have the power or capacity to), usually with the intention to subdue the victim. Researchers like Anastasia Powell & Nicola Henry (2019) have theorized that image-based sexual violence occurs within a broader pattern in gender-based intimate partner violence, and the threatening nature of the behavior may also be part of a pattern of coercive control or power exertion. Deepfake technology poses significant risk for victims of domestic violence because perpetrators can use deepfakes to threaten, blackmail, and abuse them (Kwelin, 2022).

Circumventing Consent

Like other forms of sexual abuse where the crux is the absence of consent, perpetrators of image-based sexual abuse, especially in deepfakes as we shall see below, are motivated by

the possibility of sensory simulation through AI-altered videos and aim to circumvent the need to seek and obtain consent.

Revenge

Revenge is aggression in response to intentional harm (Stuckless & Goranson, 1992). It is a counteraction perpetrated for the purpose of causing injury or harm to the victim, usually in return for an injury or wrong suffered or perceived to have been suffered at their hands. Revenge porn is the abuse of rights in the form of non-consensual intimate image dissemination (Mania, 2022). Image-based sexual abuse can be committed by an aggrieved party or an ex-intimate partner who has in their possessed or come in contact with explicit content belonging to the victim. The perpetrator then uses this content to exert revenge on the victim solely for the purpose of injury or damage to social reputation or to exert power over the victim. When a person's explicit images are distributed without permission, this can be a method of getting back at an ex-partner who chose to leave the relationship, especially where certain constraints exist which make it difficult for the perpetrator to meet directly with the victim (DeKeseredy & Schwartz, 2016). The motive is for the supposed offender to suffer as they did (Gollwitzer et al. 2011) and to be taught a lesson (Baumeister, 1997) as means of balancing the scales (McCullough et al. 2001). People may seek revenge to restore both intrapersonal and interpersonal balance (Dyduch-Hazar & Mrozinski, 2022).

In 2018, a famous YouTuber found that in a bid to exert revenge, a sexual video of her had been leaked online by her former romantic partner sometime after the end of their relationship. As a result, Chrissy Chambers developed anxiety, insomnia, posttraumatic stress disorder (PTSD), and soon began to abuse drugs to numb the pain. BBC received reports on the backlash she has had to face since the incident with several people calling her unsavory names and disassociating themselves from her (BBC 2018).

Proof of Masculinity

In an investigation into the nature and scope of image-based sexual abuse on 77 high-volume online websites, Henry & Flynn (2019) found that on the majority of these sites the users appeared to be motivated by sexual gratification and proving masculinity to a sexually deviant peer network. They used image-based sexual abuse as the vehicle to drive the agenda. The study showed that a case of publishing or sharing intimate sexual media is not as simplistic as the paradigmatic 'ex-lover' revenge narrative (Henry & Flynn, 2019).

Sextortion

The Cambridge Dictionary (2022) defines sextortion as a crime of the digital age, involving the practice of forcing someone to do something, particularly to perform sexual acts, by threatening to publish naked pictures or sexual information about them. It is the threatened dissemination of explicit, intimate, or embarrassing images of a sexual nature without consent, usually for the purpose of procuring additional images, sexual acts, or money (Patchin and Hinduja, 2020). With the abuser's threat to expose explicit content in their possession, victims of image-based sexual abuse can be blackmailed for sexual favors or monetary gain.

Injury to Social Reputation

There are instances where an offender can seek solely to cause injury to the social reputation of the victim (Pagliaro et al., 2022). An example is during a campaign of distortion where the creation and dissemination of explicit content can be done to discredit the integrity of a candidate, force a step-down, and bully them into hiding. This is usually done for personal gain, such as to better the chances of the other candidate. This is made even more worrying with the nature of today's communication environment which allows for easy and quick

dissemination, aggravating the capacity of deep fakes to cause reputational harm. The combination of cognitive biases and algorithmic boosting increases the chances for salacious fakes to circulate. The ease of copying and storing data online-including storage in remote jurisdictions also makes it harder to eliminate fakes once they are posted and shared (Chesney & Citron, 2019). This means that deepfakes are hard to recall, and it is even more difficult to control the spread, thereby increasing the chances that various persons in the victim's personal networks may come in contact with the deepfakes. This is even more devastating to the victim's future prospects of business, work and personal relations, since employers would rather hire people with less damaged reputations.

The Impact of Deepfake Technology on Image-based Sexual Abuse

Now that we have set the background and context for image-based sexual abuse and the motivations behind it, we will now explore in detail how AI technology enables an image-based sexual abuse that takes a different form in the digital sphere. To do so, we offer an overview of the meaning of AI, how this technology is used to create deepfakes through machine learning, some of the uses of deepfakes, and how this deepfake technology has been exploited for deepfake pornography.

Definition of Artificial Intelligence, Machine Learning, and Deepfakes

Artificial Intelligence is the automation of activities that we associate with human thinking, such as decision making, problem solving, and learning (Russel & Norvig, 2003). AI can take the form of machine learning, speech recognition, and virtual assistance. Merriam Webster Dictionary (2020) defines deepfake as an image or recording that has been convincingly altered and manipulated using an AI technology to misrepresent someone as doing or saying something that they did not do or say. This is achieved through deep learning, the adaptation to new circumstances to detect and extrapolate patterns through algorithms that teach themselves how to solve problems with large data sets. They are used to swap faces in videos, images, and other digital content to make the fake appear real.

How Deepfake Technology Works

One of the most important elements in deepfake technology is machine learning. This is where machines rely on a set of artificial networks called convolutional neural networks designed to mimic human intelligence. They are computational processing systems which are heavily inspired by the way biological nervous systems (such as the human brain) operate (O'Shea & Nash, 2015). They are composed of a high number of interconnected computational nodes (referred to as neurons), which entwine in a distributed fashion to collectively learn from the input in order to optimize its final output. The process of making a deepfake starts with the convolutional neural networks. It is worth noting here that a replica deepfake cannot be created without a representation of the real media in video or image form. However, in recent times, a blend of old and newly manufactured media can be used, and existing data can also be used to create new media. The video or image is then countlessly fed to a deep neural network, which would have been previously trained. Then it will begin to deconstruct the subtle features of the person's face and manipulate them based on the individual conditions of the media. Today, such rigorous processes and techniques are being replaced with applications that come fully integrated for easy creation of deepfakes and in far less time. They can also be created with only basic graphic design knowledge. Deepfake technology can result in synthetic videos, pictures, deepfake texts, and real-time deepfakes.

Uses of Deepfake Technology

Deepfakes have been used in the film industry to create clones as well as to modify and edit characters in a film as required. This replaced the former VFX technologies which were more cumbersome and required more expertise. Today, deepfakes have become an important part of filmmaking. Producers simply need to input videos and images they want to face-swap into a program designed to create deepfakes. This is then tracked and replaced by AI in a matter of minutes without the need for experts. This use of deepfakes has been seen in various blockbusters like in the *Fast and Furious* series (Diesel et al. 2017). Weta Digital (2017*)* reports that for 260 shots, a performance similar to what the late Paul Walker could have given was completed using deepfake technology. This was created using performances from Paul's brothers to give other actors the opportunity to perform and interact with them. After the set-up, their facial performances were captured in special-type cameras from which digital versions of the on-set performance were replicated. All the while, footage from previous seasons were referenced to keep the deepfakes detailed enough to maintain the integrity of the character. Post-production work on movies has long made fakes appear very realistic at the cinema (Kietzmann et al. 2020). Another example is found in *The Curious Case of Benjamin Button* (Fincher, 2008) which won the Academy Award for Best Visual Effects in 2009. The movie relied on computer-generated imagery to tell the story of a baby born with the appearance and mannerisms of an elderly man who then spends 84 years growing younger, until he transforms into an infant.

UNICEF and MIT are currently improving on a project started in 2017 called "Deep Empathy," in which AI is used to increase empathy for victims of far-away disasters by imagining what the viewers' home locations would look like under similar disaster conditions (Project Deep Empathy). This is achieved through creating digital clones and deepfakes with the intent to get the viewer closer to the realities of those that suffer the most, by helping them imagine what neighborhoods around the world would look like if hit by a disaster.

Colin Campbell et al. (2022) describe the use of deepfakes in advertising where in order to influence brand perceptions, product and service advertisers resort to altering images and videos to depict what may not be entirely true for the purpose of eliciting a response from the customers. There have been instances of political campaigns where deepfakes were used to portray candidates in a light that appealed to the masses, like President Tiwari's deepfake advert where he seemed to speak fluent Hindi.

Deepfake technology is merely a tool, and like most tools, the ethics of its use will be dependent on who wields the handle. As such, deepfake technology has also been attributed to other ills like creating child sexual abuse material, fake news and misinformation, hoaxes, bullying, financial fraud, and other harms. There have been situations where passports have been forged with a deepfake photograph which is usually difficult to detect and could then be used to facilitate other crimes like identity theft, trafficking, and illegal immigration. Also, deepfakes of embarrassing or illegal activity could be used for extortion. In organizations, phishing could move to a new level if the luring includes a video or manipulated voice of a trusted friend created by deepfakes. When a business email compromise attack is supported by a video message and voice identical to the genuine CEO, sensitive office information could be falsely elicited and used to perpetuate further financial crimes and, in extreme and more damaging cases, market manipulation. In the political space, they were used as weapons to smear and portray political figures in negative lights to better the chances of their opponents. Deepfakes were also used to propagate and incite negative emotions to sway or rile supporters in what is known as campaigns of distortion. An example is found in the 2019 video footage of President Obama swearing during a public service announcement which sparked outrage from viewers. Also, a deepfake video of Mark Zuckerberg announcing that he is deleting Facebook attracted 72 million views and led to outrage among viewers who believed the

content to be authentic. Deepfakes have earned the reputation as primary tools for both domestic and international disinformation and are capable of contributing to the social division of a nation by lowering trust in institutions and authorities while also undermining journalism and other trustworthy sources of information (Helmer, 2022). Deepfake images and videos circulating through social media and news outlets, especially of a celebrity or public figure, paves the way for misinformation, depending on the nature and intent of the deepfake. Misinformation can lead to a general distrust of news sources, government officials, institutions, or individuals. Ultimately, the rampant use of deepfakes can make the public more unsure of what is real and what is fake. Also, geopolitical tensions between nations can ensue through deepfakes.

Rajat Budhiraja et al. (2022) have found that deepfakes have made their way into the medical and health industry. A medical deepfake is where an application of AI-triggered deepfake technology has been made to medical modalities like Computed Tomography (CT) scan, X-Ray, or ultrasound by either inserting or removing certain disease conditions and tumors from the modality under analysis.

Soon, deepfake technology found its use in a rather uncanny manner in the pornography industry. Here faces of victims are masked onto other bodies in sex videos to create illusions that enable virtual sexual exploitations fueled by different motivations.

Impacts of Deepfake Pornography: AI-Enabled Sexual Abuse

Some of the popular victims of deepfake technology for virtual sexual abuse include Kate Isaacs, leader of anti-porn campaign group Not Your Porn, and Cara Hunter, a 26-year-old Northern Irish politician. Kate Isaacs is an author and a social and political activist of British background. She has instituted and carried out research into the activities and regulation of the pornography industry and has seen to the deletion of explicit content hosted on pornographic sites without the consent and age verifications of the individuals. Kate carried on with her activities as an anti-porn campaign leader for a while before she became a target for deepfake pornography herself. She gave an account of the experience which, she narrates, left her in shock for several years. Kate recalls that it had been a normal day in 2020 as she was casually scrolling through her phone, when she realized she had been trending on Twitter over an alleged porn video she had starred in, except she was not a pornography actor.

In a documentary interview with Jennifer Savin for BBC, Kate recounted that she had been in severe shock when she realized she had been a victim of deep-fake pornography. She said the motivation behind the act was to "punish" her for her values, the right fit for her "crime" as an image offense activist.

Cara Hunter, a Northern Irish politician, was another victim of deepfake pornography. During the late stages of her election campaign in 2022 and a couple of weeks before she was elected as the Social Democratic and Labour Party (SDLP) Member of the Legislative Assembly (MLA) for East Derry, Cara found that a pornographic video in which she appeared to be engaging in an oral sex act was circulating online. Cara told iNews:

> I was at a family party, it was my grandmother's 90th birthday, I was surrounded by family and my phone was just going ding, ding, ding. And over the next couple of weeks, it continued like that. I remember my cheeks flashing red and thinking, 'Who is this person? Did I have sex with this person?' Two days after the video started doing the rounds, a man stopped me in the street when I was walking by myself, and asked for oral sex (Hunter, 2022).

In 2018 Rana Ayyub, an investigative journalist and opinion columnist, was also a victim of a pornographic deepfake video which had been created maliciously to stifle her voice

and then circulated in several millions of systems in India alone. This was in addition to countless rape and death threats she received. In response, she filed a complaint with the Delhi Police, who subsequently decided to close the case in August 2020 saying that despite efforts the culprits could not be identified. It took the intervention of the United Nations to come to the aid of Ayyub (hospitalized with anxiety and heart palpitations), which then spurred actions from the Indian government and the social media actors such as the influencers, activists and well-meaning individuals. The lackadaisical attitude in response to claims of image-based sexual abuse is noteworthy. In addition to the harm caused by the perpetrators of this unique form of abuse, several instances have been met with social ridicule, or at best, indifference (Sparks, 2022).

The convincing nature of deepfakes are noted here to have successfully incited doubt in the minds of the victims themselves. Svitlana Zalishchuk, then a member of the Ukraine Parliament, Helen Mort, a poet from Sheffield, York, and Jess Davies, a former model now BBC journalist and presenter, are victims who reported that their non-explicit photographs had been taken from their social media pages and websites, manipulated, and uploaded to pornographic sites.

As with other forms of sexual abuse, image-based sexual abuse can be a major stressor with significant mental health consequences for victims. As seen above, individuals who are on the receiving end of image-based sexual abuse have made several remarks on the negative impacts the experience had on them, like Post Traumatic Stress Disorder (Bates, 2017), reclusiveness, and self-isolation.

The Position of Policy and the Law

As discussed above, the synthesis of image-based and other forms of sexual abuse ensures protection by criminalizing all forms of sexual violence. The various legislations and agreements in this regard include more comprehensive laws offering general protection from all forms of sexual abuse. This is seen on the international level with the UN Declaration on the Elimination of Violence Against Women and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). There are also national laws like the Sexual Offences Act of 2003 and The Violence Against Persons (Prohibition) Act 2015 of Nigeria, and then, more specific legislations against image-based offenses like The UK Revenge Pornography Guideline. Seonaid Stevenson & Sarai Chisala Tempelhoff (2021) note that there are conversations being had between the Scottish and Malawian Governments to ensure laws and statutes are created to criminalize gender offenses as well as discussions around the challenges Image Based Sexual Abuse presents for women and girls.

Deepfakes also raise unique issues that have warranted the reform of various laws to include provisions for its regulation. Some of these laws include the U.S. National Defense Authorization Act (NDAA) which instructs the Department of Homeland Security to study deepfake creation technology and possible detection and mitigation solutions. In May 2022, the Committee on Homeland Security and Governmental Affairs submitted a report titled "Deepfake Task Force Act: report of the Committee on Homeland Security and Governmental Affairs, United States Senate, to accompany S. 2559." This report established the Deepfake Task Force Act and the National Deepfake and Digital Provenance Task Force as the administering body. There is a more recent ratification of amendments to the Digital Services Act (DSA) by the European Parliament on criminalizing deepfakes. Also, in the state of California, two bills that were passed last year made aspects of deepfakes illegal. Assembly Bill 602 banned the use of human image synthesis to make pornography without the consent of the people depicted, and Assembly Bill 730 banned manipulation of images of political candidates within 60 days of an election. The US congress has also introduced a few more bills,

like the Malicious Deep Fake Prohibition Act of 2018 and the Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act (or the DEEPFAKES Accountability Act).

Shortcomings of the Malicious Deepfake Act

The US Malicious Deep Fake Prohibition Act has especially been criticized by many scholars for its shortcomings in being overbroad. One is American scholar Rebecca Delfino of Loyola Law School, who expressed worry for the wide approach the Act had adopted in its definition of deepfakes. Section 3805 defines a deepfake as "any audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual" (MDFPA, 2018).

Delfino (2019) advises that a definition of this type, without any limitations or modifiers, casts too broad a net to cover a lengthy range of media, including legitimate, non-offensive content like computer-generated imagery in films. The inclusion of such overbroad exemption would allow nearly every deepfake as long as the intention is not to cause harm, like in the case of a parody or satire. Compare this to the UK Revenge Pornography Guideline discussed above which made an intention to harm a requirement for a charge in image-based abuse to hold water. This could allow for a lot of leeway for such harms to be committed under various guises, irrespective of the harm caused to the individual who may not have consented to the processing of their sensitive media in such a manner. We submit that the Guideline should have made a crucial case for explicit consent of the dissemination of the content as the only defense in this case where no further evidence is produced to show a withdrawal of such consent.

The Law in Other Countries

In some other countries like Canada, deepfakes are protected by Canadian copyright laws as works of artistic expression. However, there exists a line of defense in Canadian law against deepfake pornography which is enshrined in the Canadian Criminal Code. This law protects against child sexual abuse material, the depiction of any person under the age of 18 in sexual material, and extends to electronic generated materials produced using computer means. Karasavva & Noorbhai (2020) assert that not only would the production of deepfake videos with the face of a minor fall into this category, but posting such a video would also be prosecuted as an act of distributing child sexual abuse material. To support this assertion, they also alluded to precedents where individuals who superimposed images of minors on sexual material have been charged and prosecuted under the child pornography laws.

The Creation of Deepfakes and Implications for Privacy under the General Data Protection Regulation

We will now attempt an in-depth analysis of the creation of deepfakes in light of the General Data Protection Regulation. First, there is a need to decide if the personal data as defined in the regulation is processed during the creation of deepfakes. There have been various conversations on whether the creation of deepfakes violates the provisions of the GDPR. Baran Yildrim & Celal Aydinli (2019) posit that because of the fake nature of deepfakes, consideration of data protection rules would be irrelevant because the content itself does not belong to a real individual. This might be true in some situations where a deepfake is created without inspiration from a source. When a deepfake of a person that does not exist is created using different input of personal data, the deepfake does not relate to an existing, identifiable person. This means the deepfake itself is not personal data since it cannot be traced or used to identify an actual person.

But this is not the case in situations, like in image-based sexual offending where the victim's data forms a considerable amount of content for the deepfake and the finished product is easily traced back to the victim. The definition of personal data under the GDPR as any information relating to an identified or identifiable natural person, may be construed to mean that the format in which the information is kept is immaterial so long as the information can be traced to a person. In this case, personal data is not necessarily objective and can extend to the subjective data of the individual like their opinions, memos, and judgements. Personal data in deepfakes for image-based sexual abuse involves the use of an already existing image or video of the victim. Since this data contains a face which can be used to identify the victim, it can be construed to come under the definition of personal data in the GDPR. The GDPR recognizes the existence of several privacy rights attributable to an individual. They are the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and the right not to be subject to a decision based solely on automated processing. Since we have attempted to classify deepfakes and media which forms the raw material as personal data, processing of personal images or videos needs to be subjected to the informed consent of the data subject.

Processing for the purpose of the regulation is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration" (GDPR, 2018). It is safe to deduce here that the creation of deepfakes involves a degree of altering of the original data and can be classified as an act of processing under the GDPR. For this reason, a victim of deepfake pornography can invoke the individual rights under the GDPR to prove the liability of the offender. However, the GDPR will only apply when the processing activities fall within the territorial scope. This is generally the case when controllers and processors have an establishment with activities in the European Union (EU). While this can be easily rectified with third party search engines like Google, where the identity of the offender is yet to be identified, it might be a challenge to link their activities with a particular jurisdiction. More so, since their activities do not require a physical presence to be affected, there are concerns on the viability of law as a regulator. Nonetheless, the absence of explicit consent in the processing of personal data is a violation of the provisions of the regulation that can be invoked. Also, a victim can exercise the right to be forgotten, granted to European residents in Article 17 of GDPR as the right to erasure. Under the right to be forgotten, a data subject can request that the controller of personal data (i.e., the creator, publisher, or third-party search engines that lead to the sites with deepfake pornography) delete, delink, or halt further access to the content.

Proposed Solutions for Deepfake Technology for Pornography

Regulating the Use of AI Technology for Synthetic Media

As already established above, the deepfake technology can be applied to various uses, but such use must be limited to applications that advance the legitimate interest of end-users and the general society. A human-centered artificial intelligence (HCAI) can be adopted to shift the focus in AI development from technology to people (Bingley et al., 2022). To achieve this, there is a need for legislation that reflects the position of the law on the subject. As we have seen above, changes are already being implemented to bring the law to speed with the harms of deepfake technology as well as criminalizing its illegal use for pornography. Implementing these changes will place it at par with all other forms of sexual abuse. But there remains a need for more targeted legislation to reflect the urgency and weight of the problems posed by deepfake technology, especially for image-based sexual offenses. One of such recommendations for specific legislation was proposed by Rebecca Delfino, who called for a Federal-Level Criminal statute. The Pornographic Deepfake Criminalization Act which, unlike the other laws, will be more tailored to deepfake technology for image-based sexual abuse,

enforced at the federal Level, and would strike a balance between protecting victims, punishing wrongdoers, and protecting freedom of expression. In the Act, a definition is proposed for Pornographic Deepfake to mean a specific type of deepfake wherein an individual is, or is depicted to be, engaging in sexually explicit conduct; or the naked genitals or post-pubescent…nipples of any individual are visible in an original or modified format, such as with a filter or text overlay.

The Act also emphasizes consent as the only basis for defense in the creation and/or the dissemination of explicit data:

> It shall be unlawful to knowingly use any means or facility of interstate or foreign commerce to distribute or create a pornographic deepfake (1) with knowledge or reckless disregard for; (a) the lack of consent of the individual or individuals to the use of their likeness or image in the creation or distribution of the pornographic deepfake; and (b) the harm that the distribution could cause to the individual or individuals; (c) without an objectively reasonable belief that such distribution touches upon a matter of public concern (Delfino, 2019).

With this provision, the proposed Act seeks to eliminate the perceived trivialization of deepfakes for pornography from earlier legislation where more weight is put on the intention of the creator and disseminator than on the consent and interest of the alleged victim of the crime. By the inclusion of "reckless disregard" in the Act, it is inferred that it will be sufficient to show that the alleged offender knows that the victim is unaware their data was used to create the deepfake, the victim is likely to be exposed to harm by the creation and dissemination, and that such creation will not advance any public good. Where these are established, it will be inferred that the intention of the creator is to harm.

With legislation like The Pornographic Deepfake Criminalization Act targeted specifically at deepfake technology for image-based sexual abuse, lawmakers are given the opportunity to conduct in-depth analysis into this ever-increasing perpetration of sexual abuse by offenders hiding behind their computers. Even more worrisome is that technology for creating deepfakes is becoming less technical by the day with the increasing number of mobile applications that can create deepfakes in a short span of time. This means more people are able to use this technology, which is not checked and regulated as urgently as it deserves. We run the risk of a chaotic circumvention of consent through deepfake pornography at an alarming rate. No one will need to daydream any longer when they can make their malevolent dreams come true virtually.

Enforcing Existing Laws on Image-based Sexual Abuse and Deepfake Technology

In the absence of enforcement, a law is as good as the piece of paper on which it is couched. For this reason, it will be immaterial how many laws are enacted if the implementation and enforcement of the law is not ensured. Law is enforced as a deterrent for new, existing, and intending offenders, and it provides a premise for the fulfillment of a promise by the government. Moreover, if human rights are to be truly upheld, a weak enforcement of law poses a major barrier to actualization, and non-enforcement bears the costs for a nation and the world. While we call for new legislation tailored to deepfakes for image-based offenses, we also advise that the enforcement of existing laws be given priority. The US Malicious Deep Fake Prohibition Act 2018 provides: "Any person who violates the provisions of the Act shall be (1) fined under this title, imprisoned for not more than 2 years, or both; or (2) fined under this title, imprisoned for not more than 10 years, or both, depending on the case" (MDFPA, 2018). The proposed Pornographic Deepfake Criminalization Act amends this to be tailored-specific to deepfakes as well as widen the scope of its application:

> Any person who violates the provisions under this title… shall be imprisoned for no more than 5 years, or both; (2) fined under this title, imprisoned for no more than 10 years, or both, in the case of a second or subsequent violation; or (3) fined under this title, imprisoned for no more than 10 years, or both, in the case of a violation where any individual depicted in the deepfake is a minor (Delfino, 2019).

The examples above of penalty sections expose the weight of the offense through the weight of its punishment. It is in the threat of penalty that deterrence, respect for human rights, national safety, and global development are achieved. In this case, image-based sexual offenses made possible by AI technology will be better curtailed if more offenders are punished under stricter and relevant laws. When a victim is a citizen or resident of an EU member nation, an application of the General Data Protection Regulation can be invoked to elicit liability for wrongful processing of personal data in the absence of explicit consent. Also, the right to erasure (or to be forgotten) under the regulation can be used as an action of redress.

Concerns in Employing Law as a Regulator

While we posit law as a regulator, we also understand the proposed difficulties that could be encountered in implementation. One of such difficulties is in attribution. A law is only an effective regulator where there is a named perpetrator. In this instance, a law can only protect victims when the creators of the pornographic deepfakes can be easily found. And with the current technological tools that help to generate anonymity in the face of crime, it will be rather difficult to bring the abusers within the ambit of the law. Of all the victims discussed above, there has been little progress in tracking and finding the abusers. Some of these abusers go to great lengths to shroud their IP addresses, which evades tracking by injecting the video into social media where widespread use will create difficulty finding the source. The attribution problem arises in the first instance because the metadata relevant for ascertaining a deepfake's provenance might be insufficient to identify the person who generated it (Chesney & Citron, 2019). The expensive nature of civil suits, which must be borne by the victim, will necessitate the input and intervention of non-governmental organizations to ameliorate. The global nature of digital technology creates a utopia for criminals where the hands of the law are tied. It is difficult to apply the law of a particular jurisdiction when seeking redress for deepfake pornography if the perpetrator is a citizen or resident in another jurisdiction. This is especially challenging when the deepfake technology abuse is not prohibited or criminalized in the second jurisdiction in question.

Raising Public Consciousness

Due to the wide-spread availability of tools to create deepfakes, it is imperative that the public be made more aware of the dangers of the deepfake technology as a form of ax-grinding, trolling, and damaging social reputation. This is of utmost importance in the current age of social media where people constantly share personal data that can be harvested and manipulated for a plethora of wrongs. Cases like The Cambridge Analytica have shown us that while we may expect that data shared online is used the way users intend, some data are being siphoned to other uses without consent. The need for data privacy is currently at an all time high because of the new ways our data could be used against us. While laws and regulations like the General Data Protection Regulation attempt to control how data is harvested, stored, and processed, it is imperative that people are aware of which pieces of their data can be made public. This in itself may not erase completely the perpetration of crimes against data, but nonetheless, can be a start for individuals to take this reality more seriously.

In addition, law enforcement and the judiciary must stay abreast of technological trends as rapidly as they evolve. They should also receive specialized training in technology and its offshoots like AI and information security education for cybersecurity. Awareness of the dangers of cyberbullying as well as sensitivity training is also necessary. Among legal scholars, more interdisciplinary approaches to the challenges posed by technology are necessary.

Survivor Support and Advocacy

Kate Isaacs, Cara Hunter, and Holly Jacobs each state that the most difficult part of being a survivor of image-based sexual abuse through deepfake pornography is integrating back into a society that is prone to consume media without discerning legality. We noted earlier how convincing deepfake technology must be that even the survivors themselves experience moments of doubts. Building back social reputation is a daunting task in itself and survivors need as much support as they can find. Currently, there are a number of organizations all over the world with missions to provide support to survivors of cyberbullying and abuse. Some of these organizations include the Cyber Civil Rights Initiative (CCRI), founded by Holly Jacobs after she became a victim of sexual abuse through deepfake pornography. CCRI is dedicated to combating online abuses that threaten civil rights and civil liberties, spreading awareness, and providing support for survivors of image-based sexual abuse. More organizations of this nature should be encouraged to bring all hands on deck.

Technology Should Be Used to Clean up its Own Mess

As a technology tool, AI will sometimes be used unethically. We can find recourse within the same technology to solve some of the hazards caused by its misuse. An opportunity for this is found in AI-powered detection software. In this process, the same techniques used to make deepfakes can detect evidence that a picture or video has been tampered with. Another way technology can be harnessed is through watermarking information. This is the direct embedding of additional information or a host signal into the original content (Podilchuk & Delp, 2021). This is used to detect manipulation by producing secret keys on the host data. One cryptographic device is the Amber Authenticate which is used to produce hashes at predetermined intervals throughout a movie, so that when an alteration of the video is made, this will be detected in the rearrangement of the hashes and the viewer will be alerted accordingly. Blockchain technologies can also be explored for additional security (Jing & Murugesan, 2021). Blockchain is a tamper-evident and tamper-resistant digital ledger implemented without a central repository to enable communities of users to record transactions in a shared ledger. Under normal operation of the blockchain network, no transaction can be changed once published (Yaga et al. 2019). This means that blockchains are resistant to a wide range of security vulnerabilities that centralized data storage is susceptible to. While it may not store large data, the cryptographic keys can be stored using blockchains. Furthermore, by enabling provenance and traceability of digital content, blockchain technology can help to create an audit trail for digital content. Xiangling Ding et al. (2022) propose a two-stream method to capture the spatial-temporal inconsistency cues found in deepfakes and interactively fuse them to detect deepfake videos. They note that the traces of spatial inconsistency in deepfake video frames mainly appear in their structural information, which is reflected by the phase component in the frequency domain. The proposed frame-level stream learns the spatial inconsistency from the phase-based reconstructed frames to avoid fitting the content information. We believe that only technology can know technology well enough to regulate technology for good uses. For this reason, in addition to the above proposals, we encourage a "safety by design and architecture approach" to regulating deepfakes where the system and technology can only be used for the legal purposes for which they were intended. Other uses in non-conformance will be made impossible *ab initio* (from scratch). We also understand that

the challenges of technology as a solution are daunting due to the rapid innovations in deep-fake technology which a detection software would have to keep pace with. While we cannot trust that technology will deliver a reliable approach to minimize the harms deepfakes might cause, we argue that technology could be a start in ensuring its curb in the first instance.

Web Hosts and Platforms for Content

While certain laws like Section 230 of the Communications Decency Act (CDA) provide an immunity from liability to online platforms who host user-generated content for harmful content uploaded on their sites, they are still expected to act in good faith and ensure safety. Fortunately, most web hosts and social media platforms have begun to prioritize regulation of content to ensure that rules, guidelines, and principles are adhered to. One of these measures is the Instagram Community Guidelines against the publishing of X-rated or explicit content to make the platform safe for all to use. These platforms are advised to engage stricter privacy controls as well as provide mechanisms to automatically take down abusive content like revenge porn that violate the site's terms of service. Also, reports of disturbing content and takedown requests by victims of deepfakes (or any concerned party) should be given swift attention due to the sensitive nature of the request. It is important that the request is not limited to being brought by the victim only. There have been cases where the victim's attention was brought to the content later on. In these circumstances, it would be counter-intuitive to request the sole authorization for a takedown by the victim while the content continues to be disseminated.

Conclusion

As the physical world continues to fuse with the digital space, now is the time to prioritize conversations on the ill use of deepfakes as one of the by-products of technology and its manipulation for pornography and image-based sexual abuse. While scholars and victims call for stricter laws to eradicate the use of deepfake technology for pornography, policy makers should respond by increasing productive conversations on these specific legislations. Due to the increasing rate of technological advancement and the delay in reforms, the law should not function alone as the only regulatory mechanism to curb malicious deepfake use. Digital education should be made a norm in the new digital era. There is a need for individuals to adopt a calculated and reasonable approach to dissemination of personal data to maintain data privacy in light of the dangers of this technology. More worrisome is the increasing technical inability required to create deepfakes with the wide range of mobile applications that generate convincing clones which cast doubts in the mind of the victims themselves. Codes and technology can be employed to curtail the malicious use of deepfakes by implementing a safety-by-design approach in the design of deepfake technologies. Content platforms and web hosts can also ensure their policies are constantly upgraded to regulate third party content uploaded on their platforms as well as adopting every viable means to protect users. Finally, all collaborative efforts for safety and support must be encouraged.

References

Baumeister, R. F. (1997). *Evil: Inside Human Cruelty and Violence.* Holt Paperbacks.

Bates, S. (2017). *Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors.* Feminist Criminology.

Bingley, W., Curtis, C., Lockey, S., Bialkowski, A., Gillespie N., Haslam, A., Ryan, K., Steffens, N., Wiles, J., & Worthy, P. (2022). Where is the human in human-centered AI? Insights from developer priorities and user experiences. Computers in Human Behavior, *141*. https://doi.org/10.1016/j.chb.2022.107617

Budhiraja, R., Kumar, M., Das, M., Bafila, A., & Singh, S. (2022). MeDiFakeD: Medical Deepfake Detection using Convolutional Reservoir Networks. *IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT)*, pp. 1-6, doi: 10.1109/GlobConPT57482.2022.9938172.

Burrell, J., & Fourcade, M. (2021). The society of algorithms. *Annual Review Sociology, 47*, 213-237. https://doi.org/10.1146/annurev-soc-090820-020800.

Campbell, C., Plangger, K., Sands, S., & Kietzmann, J. (2022). Preparing for an Era of Deepfakes and AI-Generated Ads: A Framework for Understanding Responses to Manipulated Advertising. *Journal of Advertising, 51*(1), 22–38. https://www.tandfonline.com/doi/full/10.1080/00913367.2021.1909515.

Chesney, B., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review, 107,* 1753-*1819.* https://scholarship.law.bu.edu/faculty_scholarship/640.

S.2559 – 117th Congress (2021-2022): Deepfake Task Force Act. (2022, May 24). https://www.congress.gov/bill/116th-congress/senate-bill/300

DeKeseredy, W. S., & Schwartz, M. D. (2016). Thinking sociologically about image-based sexual abuse: The contribution of male peer support theory. *Sexualization, Media, & Society, 2*(4*)*. https://doi.org/10.1177/2374623816684692

Ding, Z., X., Zhang, & W., Dengyong. (2022). DeepFake Videos Detection via Spatiotemporal Inconsistency Learning and Interactive Fusion. *IEEE*, 425-433 doi: 10.1109/SECON55815.2022.9918605

Dyduch-Hazar, K., & Blazej Mrozinski. (2022). The satisfaction is mine: revenge seeking following extrinsic reward. *Journal of Social Psychology, 163*(1), 52-61. https://doi.org/10.1080/00224545.2022.2090309

Fido, D., Rao, J., & Harper, A. (2022). Celebrity status, sex, and variation in psychopathy predicts judgements of and proclivity to generate and distribute deepfake pornography. *Computers in Human Behavior, 129*. https://doi.org/10.1016/j.chb.2021.107141

General Data Protection Regulation, 2016, Regulation (EU) 2016/679.

Gollwitzer, M., Meder, M., & Schmitt, M. (2011). What gives victims satisfaction when they seek revenge? *European Journal of Social Psychology, 41*(3), *364-374.* https://doi.org/10.1002/ejsp.782

Greig, J. (2021, April 20). *How AI is being used for COVID-19 vaccine creation and distribution.* TechRepublic. https://www.techrepublic.com/article/how-ai-is-being-used-for-covid-19-vaccine-creation-and-distribution/.

Henry, N. & Flynn, A. (2019). Image-Based Sexual Abuse: A Feminist Criminological Approach. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (1109-1130). Springer.

Henry, N., & Flynn, A. (2019). Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. *Violence Against Women, 25*(16), 1932–1955, https://doi.org/10.1177/1077801219863881

Jing, T., & Murugesan, R. (2021). Protecting Data Privacy and Prevent Fake News and Deepfakes in Social Media via Blockchain Technology. In *Advances in Cyber Security.* Communications in Computer and Information Science.

Karasavva, V., & Noorbhai, A. (2020). The Real Threat of Deepfake Pornography: A Review of Canadian Policy. *Cyberpsychology, behavior and social networking, 24*(3), 203-209. doi: 10.1089/cyber.2020.0272

Karasavva, V., & Forth, A. (2022). Personality, Attitudinal, and Demographic Predictors of Nonconsensual Dissemination of Intimate Images. *Journal of Interpersonal Violence, 37*(21-22). https://doi.org/10.1177/08862605211043586.

Kietzmann, J., Linda, W., McCarthy, L., & Kietzmann, T. (2020). Deepfakes: Trick or treat? *Science Direct, 63*(2), 135-146. https://doi.org/10.1016/j.bushor.2019.11.006

Li, Y., Yang, X., Sun, P., Qi, H., & Lyu, S. (2019). Celeb-DF: A new dataset for deepfake forensics. *arXiv*, 4. https://doi.org/10.48550/arXiv.1909.12962

Mania, K. (2022). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. *Trauma, Violence, & Abuse, 23*(5). https://doi.org/10.1177/15248380221143772

Malicious Deep Fake Prohibition Act of 2018, S.3805, 115th Congress (2017-2018).

McCullough, M. E., Bellah, C. G., Kilpatrick, S. D., & Johnson, J. L. (2001). Vengefulness: Relationships with forgiveness, rumination, well-being, and the big five. *Personality & Social Psychology Bulletin, 27*(5), 601-610. https://doi.org/10. 1177/0146167201275008

McGlynn, & Rackley, E. (2017). Image-Based Sexual Abuse. *Oxford Journal of Legal Studies, 37*(3), 534-561. https://doi.org/10.1093/ojls/gqw033

O'Shea, K., & Nash, R. (2015). An Introduction to Convolutional Neural Networks. *Arxiv, 2*, 1-11. https://doi.org/10.48550/arXiv.1511.08458

Pagliaro, S., Cavazza, N., Paolini, D., Teresi, M., Johnson, J., & Giuseppina, P. (2022). Adding Insult to Injury: The Effects of Intimate Partner Violence Spillover on the Victim's Reputation. *Violence Against Women, 28*(6-7), 1523-1541. doi: 10.1177/10778012211014566.

Patchin, J., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse, 32*(1) https://doi.org/10.1177/1079063218800469.

Podilchuk, C., & Delp, E. (2001). Digital watermarking: algorithms and applications. *IEEE Signal Processing Magazine, 18*(4), 33-46. doi: 10.1109/79.939835

Powell, A., & Henry, N. Technology-Facilitated Sexual Violence Victimization: Results From an Online Survey of Australian Adults. *Journal of Interpersonal Violence, 34*(17). https://doi.org/10.1177/0886260516672055

Project Deep Empathy (2018). Massachusetts Institute of Technology. https://www.media.mit.edu/projects/deep-empathy/overview/

Ringrose, J., Milne, B., Mishna, F., Regehr, K., & Slane, A. (2022). Young people's experiences of image-based sexual harassment and abuse in England and Canada: Toward a feminist framing of technologically facilitated sexual violence. *Women's Studies International Forum, 93. https://doi.org/10.1016/j.wsif.2022.102615*

Russel, S., & Norwig, P. (2020). *Artificial intelligence: A modern approach*. Prentice Hall.

Saleh, Z. (2021). Artificial Intelligence Definition, Ethics and Standards. *The British University in Egypt*. https://www.wathi.org/artificial-intelligence-definition-ethics-and-standards-the-british-university-in-egypt-2019/

Sparks, B. (2022). A Snapshot of Image-Based Sexual Abuse (IBSA): Narrating a Way Forward. *Sexuality Research and Social Policy, 19*, 698-704. https://doi.org/10.1007/s13178-021-00585-8

Stevenson, M., & Tempelhoff, C. (2021). Image-Based Sexual Abuse: A Comparative Analysis of Criminal Law Approaches in Scotland and Malawi. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse.* (513-532). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211038

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain Technology Overview. *Arxiv.* https://doi.org/10.48550/arXiv.1906.11078

Yildrim, B., & Aydinli, C. (2019). Deepfake: An Assessment From The Perspective Of Data Protection Rules. *Actecon.*