Deepfakes: An EU and U.S. perspective

Fake images, sounds and videos are nothing new – but it does not take a whole editing suite to create them anymore. The volume of deepfake videos and images online is rising rapidly, raising questions around their use in hoax-led scams, fake news and electoral manipulation. How to prevent their misuse forms part of a wider debate around how to tackle disinformation and fake news online. In this article we look at what is being done and what can be done in Europe and the U.S. to stop the rise of deepfakes.

What is a deepfake?

A deepfake is video or audio content which has been manipulated using artificial intelligence to make it appear that a person is doing or saying something which is not real. For example, face replacement or "face swapping" involves stitching the image of someone else's face over another and speech synthesis involves modelling someone's voice, so that it can be used in a video to make someone appear they are saying something they are not.

Whilst deepfakes have been used to great effect in the film and advertising industry, for improved CGI, there has also been a growing misuse of deepfakes. To date, the most prevalent use of deepfakes is face replacement pornography, where the likeness of an individual, most often a celebrity, has been used in conjunction with a porn star's body. This can result in great distress to the target celebrity or other individual. Reported examples range from fake videos of Kim Kardashian, to 'living portraits' of the Mona Lisa or Salvador Dali, and even images of people who do not exist. There has also been a growing use of deepfakes for fake videos of politicians, which has the potential to be extremely disruptive on a very large scale, for example, distorting political elections or manipulating public opinion. Although the technology is not sophisticated enough yet for it to be impossible to detect a deepfake, the technology is constantly improving.

Tackling deepfakes in Europe

There are currently no European laws or national laws in the UK, France or Germany specifically dedicated to tackling deepfakes. The EU Commission aims to tackle online disinformation in Europe, including the use of deepfakes, by way of a series of measures, including a self-regulatory Code of Practice on Disinformation[9] for online platforms. The Code includes commitments such as, amongst other things, ensuring that services have safeguards against disinformation and easily-accessible tools for users to report disinformation. However, the primary aims of the Code are targeted at the problem of fake news online rather than deepfakes. The Commission said

that, before the end of 2019, it will assess the effectiveness of the Code based on the actions taken by signatories over the past 12 months. This is therefore a developing area.

Similarly, in the UK, the Government's Online Harms White Paper, published in April 2019, acknowledges deepfakes in the context of AI being used for disseminating false content and narratives but does not specifically single them out as a policy area. The paper's proposal of a statutory duty of care on companies to increase their responsibility with regards to users' safety and to address harm caused by online services' content or activity generally could apply to some of the negative impacts of deepfakes but this is currently only a recommendation and has yet to be developed.

What existing laws might help?

Existing laws in the UK, France and Germany may help in specific individual cases. For example, national laws on defamation can be of assistance where a deepfake has been used to present an individual (or company) in a way that could harm their reputation. Deepfakes are also often created by using multiple images of a person, which are then used to train the AI to reconstruct that person's face. In these instances, the underlying source images may be protected by copyright and the photographer may also have moral rights in the images, such as, in France, the right not to have one's work altered without consent or, in the UK and also Germany, the 'right to object to derogatory treatment' of a work. However, the right to bring an action for copyright infringement or breach of moral rights lies with the copyright owner or author of the image and that may not be the subject of the image: the person targeted by the deepfake.

> Whilst deepfakes have been used to great effect in the film and advertising industry, for improved CGI, there has also been a growing misuse of deepfakes.

In contrast to the position in other countries, in the UK there is no 'privacy' or 'image rights' law protecting a person's image. If a person wants to prevent the use of their image, they have to rely on a patchwork of causes of action including passing off, copyright, misuse of private information and data protection. In certain circumstances, use of a person's image without consent could amount to a kind of false endorsement of products. For example, Top Shop's use of Rihanna's image on a T-shirt without her permission was unlawful. In France, on the other hand, judges do recognize the right to one's image ("droit à l'image"), which includes likeness, voice, photograph, portrait or video reproduction. Under German law, the general right of personality and the German law on artistic copyright also protect one's image. The general right of personality in addition also grants protection to the right to one's own words, the right to self-expression and the right to sexual self-determination which may also be affected by deepfakes. The person whose personality rights are found to have been infringed by deepfakes is entitled to claims for, amongst others, cease and desist, removal and financial compensation. However, even in countries such as France and Germany, which have protection for image and other personality rights, whether or not an action would be successful depends very much on the facts, and remedies will be specific to an individual in a particular case. It is therefore challenging, on the basis of existing civil laws in the UK, France and Germany to deter the fraudulent use of deepfakes in general.

Criminal Offences

Criminal laws in Europe could be a more effective general deterrent. For example, laws on harassment in the UK. In France, the French Criminal Code punishes the publication of a montage made with the words or the image of a person without his/her consent, if it is not obvious that it is a montage or if the fact that it is a montage is not clearly stated. The party receiving the deepfake material and publishing it could be exposed to sanctions unless it can establish that it genuinely believed the material was not a montage. Digital identity theft also punishes the impersonation of third parties or the use of their data to disturb the peace or to damage their reputation. This offence could be a more interesting tool to address some of the issues related to deepfakes. German criminal law, in particular, also prohibits the unauthorized distribution of videos or images, also including montages, if these are likely to cause considerable damage to the reputation of the person depicted. Deepfakes therefore can already be sanctioned under certain preconditions. The main problem for the prosecution, however, remains the necessary identification of the disseminator.

Tackling deepfakes in the United States

In the United States, several states have passed legislation in the last year to curb the harmful use of deepfakes. However, this legislation is heavily checked by First Amendment rights of free speech, and it remains to be seen whether courts will find this state-level legislation to run afoul of Constitutional principles.

In 2019, California prohibited the use of deepfakes in election materials by specifically forbidding the malicious production or distribution of

"materially deceptive" campaign materials within sixty days of an election. Effective until 2023, doctored images are considered deceptive if a reasonable person would have a fundamentally different understanding or impression of the content than that person would have of the original, unaltered image. Notably, media that constitutes satire or parody is exempt from the prohibition, as are news broadcasts publishing the images as part of a bona fide news story, internet websites, and regularly published periodicals, provided that the distribution is accompanied by a clear acknowledgement, depending on the circumstances, that the image is inaccurate or there are questions about the image's authenticity. The California legislation also contains a broad exception for broadcasting stations paid to broadcast materially deceptive media, regardless of whether the broadcasting station issues an acknowledgement regarding lack of authenticity.

In the same year, in an effort to regulate the use of pornographic deepfake images, California granted a specific right to civil damages to individuals depicted in sexually explicit materials without the individual's consent, regardless of whether the depicted individual did not actually participate in the creation or development of the materials.

The state of Virginia, likewise, amended its laws that criminalize the unauthorized distribution of sexually explicit materials with the malicious intent, in order to include the distribution of modified images with the intent to depict an actual, recognizable individual. Texas, too, has specifically criminalized the use of deepfakes, but only in the context of political elections, where an individual creates or distributes a "deep fake video" with the intent to injure a political candidate or influence the result of an election. In both Virginia and Texas, violation of the deepfakes law is a criminal misdemeanor, and could result in incarceration.

Other states have proposed, but not yet passed, legislation prohibiting the use of deepfakes in certain contexts. A pending bill in Maryland targets the use of deepfakes to influence political elections, similar to existing California law. If passed, the Maryland legislation would prohibit influencing (or attempting to influence) voters' decisions regarding whether to vote, and who to vote for, by distributing a deepfake online within 90 days of an election. Legislation introduced in Massachusetts would expand the state's existing identity fraud laws, making it a crime to create or distribute a deepfake in connection with conduct that is already considered to be criminal or tortious under existing law.

While New York has not yet considered a law specifically targeting deepfakes, it is currently considering legislation that would protect an individual's digital likeness for 40 years following their death and would allow family members to register to control a deceased individual's digital likeness.

At the federal level, Congress has enacted legislation facilitating the gathering of information regarding deepfakes and is currently evaluating additional laws that, if passed, would require further research and reporting on deepfake media and the technologies used to generate deepfakes.

> It would not be surprising if industry end up creating the sharpest weapons in the armoury to combat deepfakes, as technology is likely to develop faster than the law in this area.

For example, The Identifying Outputs of Generative Adversarial Networks (IOGAN) Act, which was passed by the House of Representatives in December 2019 and is now under Senate review, would require the National Science Foundation and the National Institute of Standards and Technology to support research on "generative adversarial networks", which are software programs that are used to generate deepfakes. Other pending legislation would, if passed, require the Department of Defense to study "the potential for the cyberexploitation of misappropriated images and videos" of members of the U.S. armed forces and their families and the Department of Homeland Security to report annually on digital content forgery technologies (defined as technologies used to fabricate or manipulate audio, visual, or text content with the intent to mislead).

While these pending laws are intended to help Congress enhance its understanding of deepfakes and the technologies used to generate them, they do not specifically regulate the use of deepfake media.

However, in June of 2019, a controversial bill that would require a creator of a deepfake to disclose that the media has been altered was introduced in the House of Representatives. Under the DEEPFAKES Accountability Act, any person who produces a deepfake would be required to include a digital watermark on the deepfake indicating that the media was manipulated, as well as an audio or visual disclosure of the manipulation. Any failure to make the required disclosures, or any removal of the disclosures, would result in a civil penalty of up to $150,000 per instance, and the legislation would make it a criminal offense to omit or remove the required disclosures knowingly and with malicious intent. The law would also create a private right of action enabling any individual or entity whose likeness is used in a deepfake to bring a civil suit if the deepfake does not include appropriate disclosures, or if the disclosures are removed.

The bill has been criticized on grounds that those who currently disseminate malicious or deceptive deepfakes are likely to continue to do so on an anonymous basis and avoid detection (and therefore liability under the prospective law). Some also argue that the law, if passed, could discourage creation of deepfakes for positive uses (e.g., satire or entertainment) that are protected by the First Amendment.

What other U.S. laws might help?

In the United States, false advertising laws, copyright protections, privacy regulations, and right of publicity laws, as well as causes of action in the form of defamation and intentional infliction of emotion distress, have been used to regulate deepfakes. Many of these existing laws, however, have shortcomings that easily render a victim without recourse. For example, regulating deepfakes via tort law or copyright infringement law has the shortcoming of often requiring that the victim portrayed in the image to have the resources – including the time – to bring a suit across jurisdictions and, potentially, against many different perpetrators, and that the victim be able to identify the perpetrator(s) in the first place.

Relatedly, Section 230 of the Communications Decency Act gives providers and users of "interactive computer services" immunity from most liability for the information provided by other information content providers. This means that frequently victims may not have a clear path to identifying the perpetrator of a deepfake image, nor would they be able to bring suit against, for example, a social media or other content-sharing platform, in order to control use of such media.

Finally, use of any U.S. law to regulate deepfakes will come under First Amendment scrutiny, meaning any regulation – existing or in the works – must be tailored to apply only to instances of actual malice or reckless disregard, and where the material is not newsworthy.

What is industry doing?

The main players in the social media industry have started to take action. For example, some platforms have added into their terms of use a strict ban on using deepfakes or any deceptive practices. Several companies have also created their own deepfake database, making it freely available to be used for synthetic video detection techniques. More decisively, a joint initiative driven by the tech giants has been launched: "The Deepfake Detection Challenge" which rewards with USD 10 million any registered and pre-screened participant who successfully develops a deepfake detection solution. The Pentagon's Defense Advanced Research Project Agency is also actively researching solutions to combat deepfakes by creating its own deepfakes, then developing technology that can identify them.

Final thoughts

As the technology rapidly evolves and improves, we expect legislators to turn their attention to regulating deepfakes, as part of the global crisis of fake news. However, it would not be surprising if industry end up creating the sharpest weapons in the armoury to combat deepfakes, as technology is likely to develop faster than the law in this area. After all, it is in the interests of companies and businesses to win the battle against fake news and information and there is money to be made in offering the tools to combat it.

Penelope Thornton
Senior Knowledge Lawyer, London
T + 44 20 7296 5665
penelope.thornton@hoganlovells.com

Patrick Fromlowitz
Counsel, Hamburg
T +49 40 4199 3332
patrick.fromlowitz@hoganlovells.com

Aissatou Sylla
Senior Associate, Paris
T +33 1 53 67 46 97
aissatou.sylla@hoganlovells.com

Rachel Fleeson
Associate, Northern Virginia
T + 1 703 610 6185
rachel.fleeson@hoganlovells.com

Margaret K Pennisi
Associate, Northern Virginia
T +1 703 610 6167
margaret.pennisi@hoganlovells.com